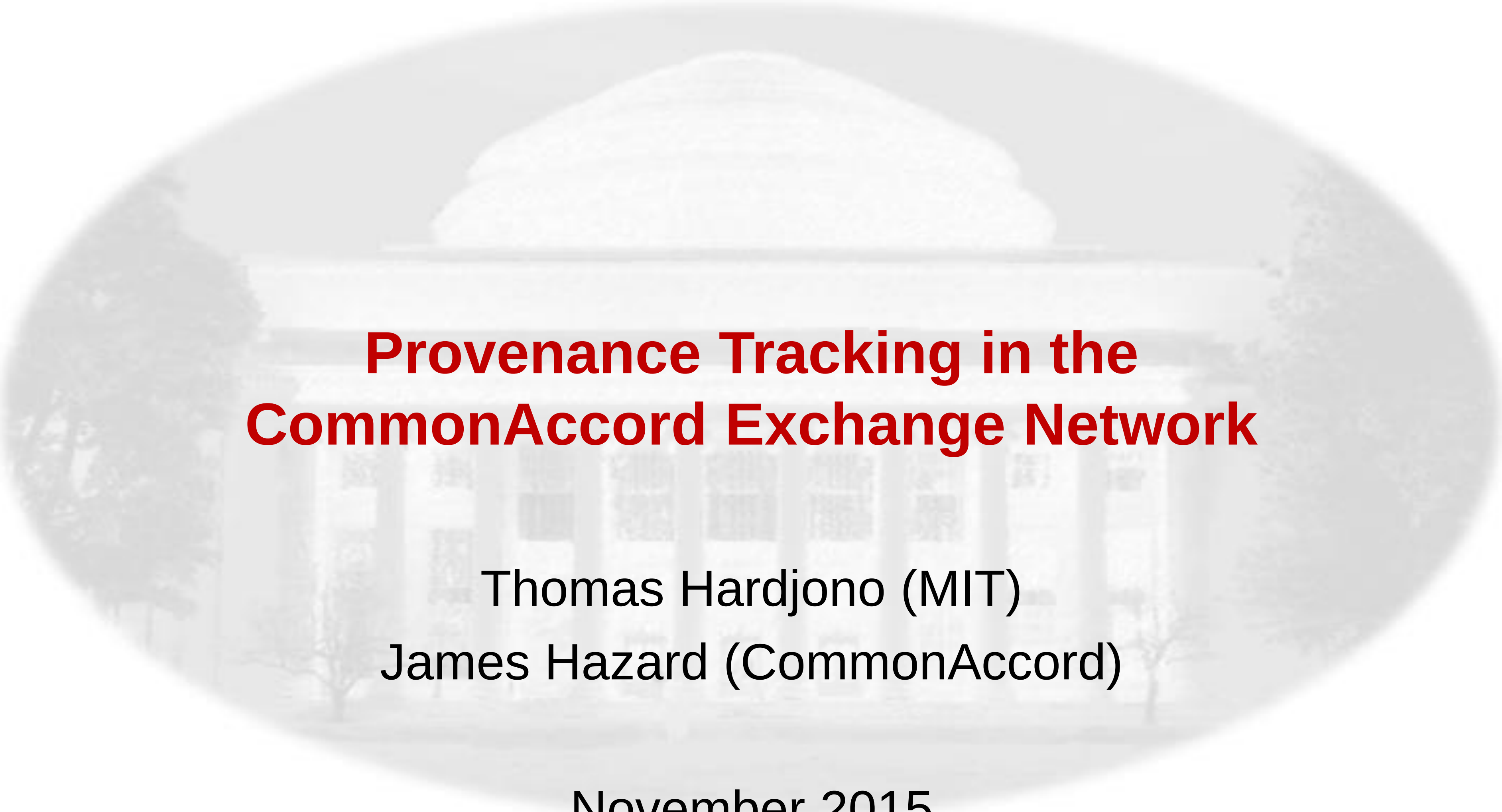


Provenance Tracking in the CommonAccord Exchange Network

Thomas Hardjono (MIT)
James Hazard (CommonAccord)

November 2015

Problem & Proposed Solution

- Problem:
  - No mechanism to track provenance of digital contracts exchanged between machines
  - No method for verifying non-repudiation beyond digital e-signatures on contracts
  - Weak method to sharing versions of contracts among negotiating parties
- Solution:
  - Enhance CommonAccord architecture with hash-chains for tracking state of negotiated contracts
  - Publish hash-chains to ledger (public or private)
  - Provide mechanism for parties to access private repositories containing contracts

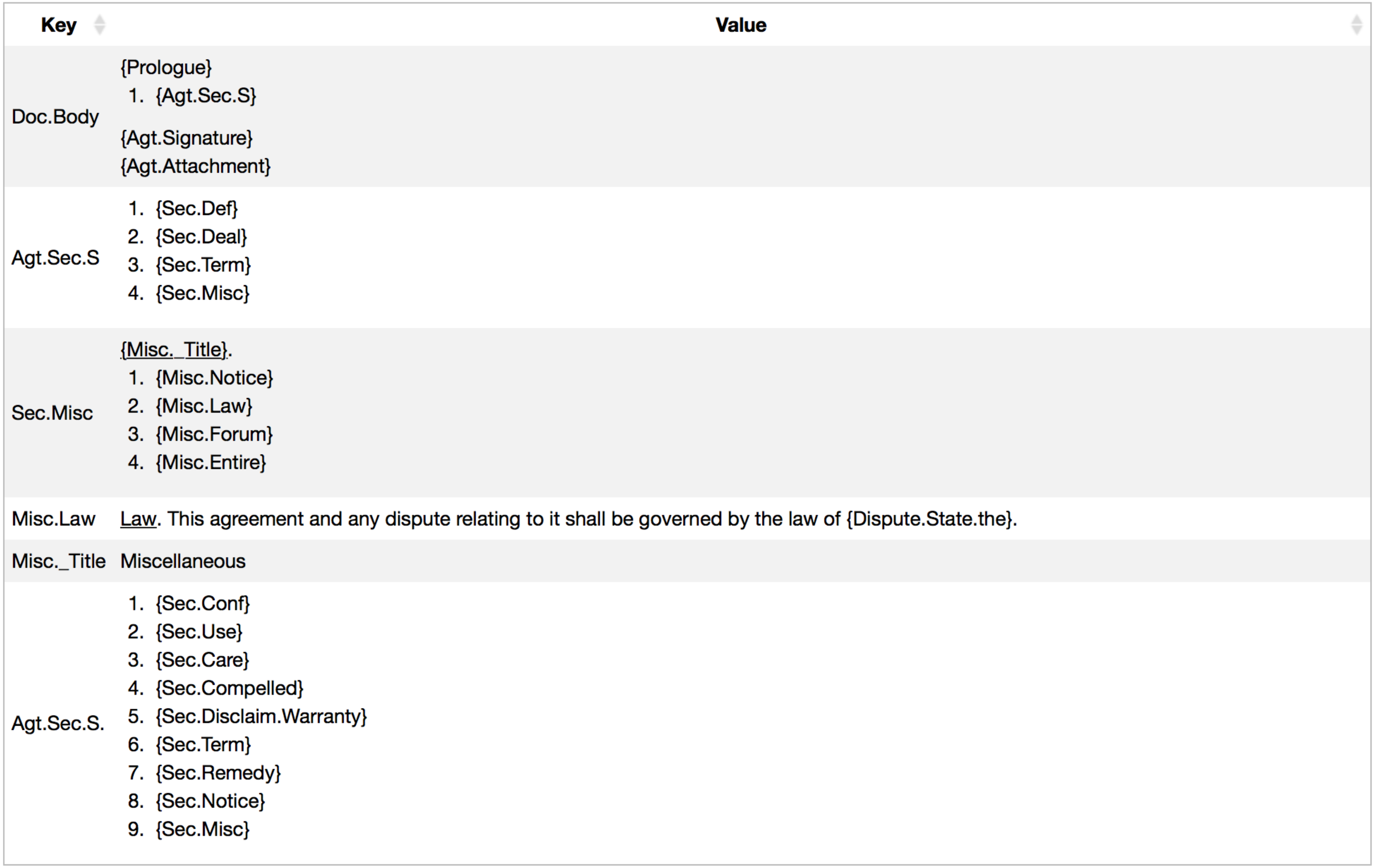
CommonAccord: Why

- Legal documents are mostly handled as text blobs, in a complex, semi-proprietary format.
- Authoring, reviewing, sharing, managing are all difficult.
  - Establishing provenance is often impossible
- The impact is delay, cost, risk, fear, imbalance, and a systemic advantage for large actors.

CommonAccord: Document as Decentralized Law

- Contracts and other party-agreed documents are decentralized legislation – which is good.
- There is a large ecosystem of persons close to the problems and capable of “mining” documents for legal conformance
  - Lawyers, among others
  - But our tools have been amazingly inefficient.
- A few source-code management methods can be used to change all of this:
  - Modularity; Versioning; text as Key/Values; prototype Inheritance; GitHub

CommonAccord: Modular Contract Components



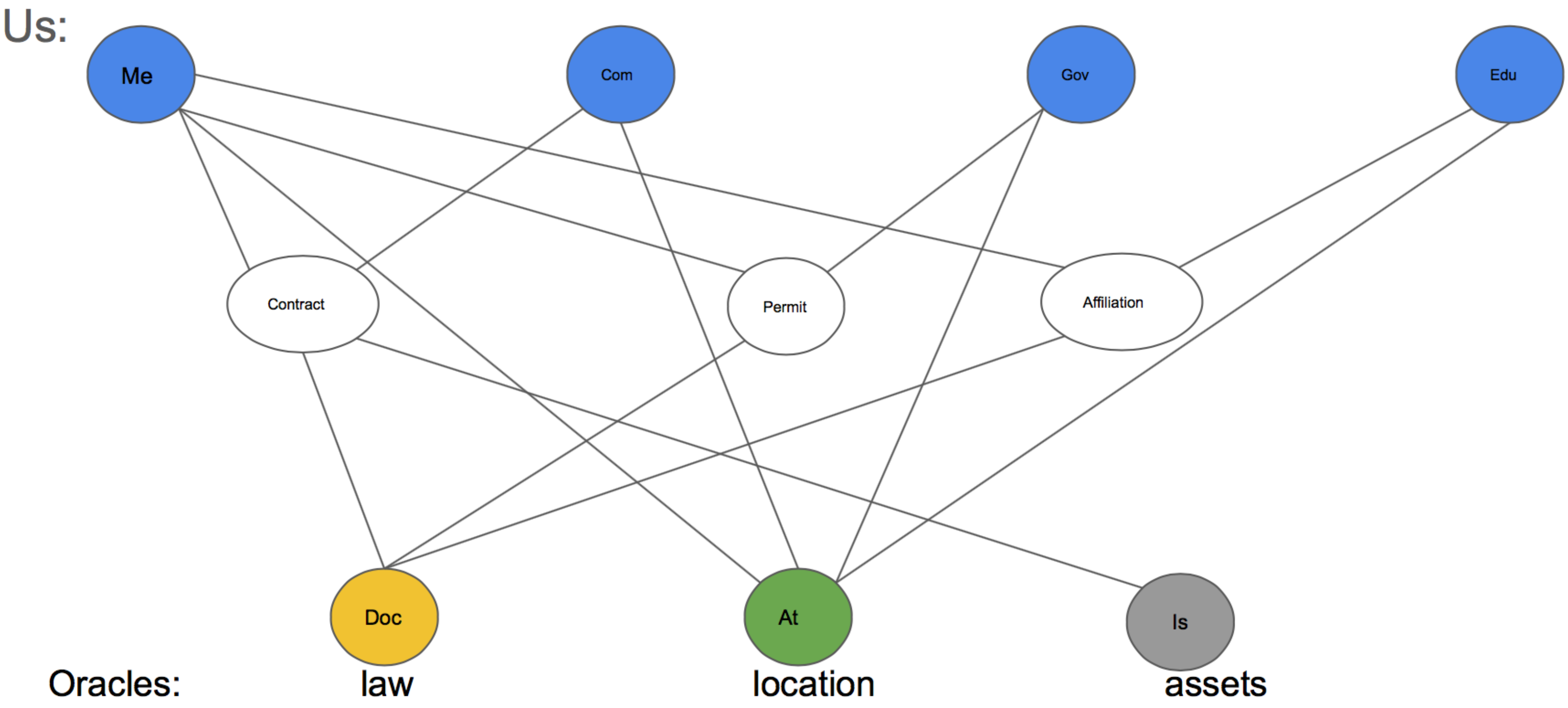
Key	Value

Doc.Body	{Prologue}
	1. {Agt.Sec.S}
	{Agt.Signature}
	{Agt.Attachment}

Agt.Sec.S	1. {Sec.Def} 2. {Sec.Deal} 3. {Sec.Term} 4. {Sec.Misc}
Sec.Misc	{Misc._Title}. 1. {Misc.Notice} 2. {Misc.Law} 3. {Misc.Forum} 4. {Misc.Entire}
Misc.Law	Law. This agreement and any dispute relating to it shall be governed by the law of {Dispute.State.the}.
Misc._Title	Miscellaneous
Agt.Sec.S.	1. {Sec.Conf} 2. {Sec.Use} 3. {Sec.Care} 4. {Sec.Compelled} 5. {Sec.Disclaim.Warranty} 6. {Sec.Term} 7. {Sec.Remedy} 8. {Sec.Notice} 9. {Sec.Misc}

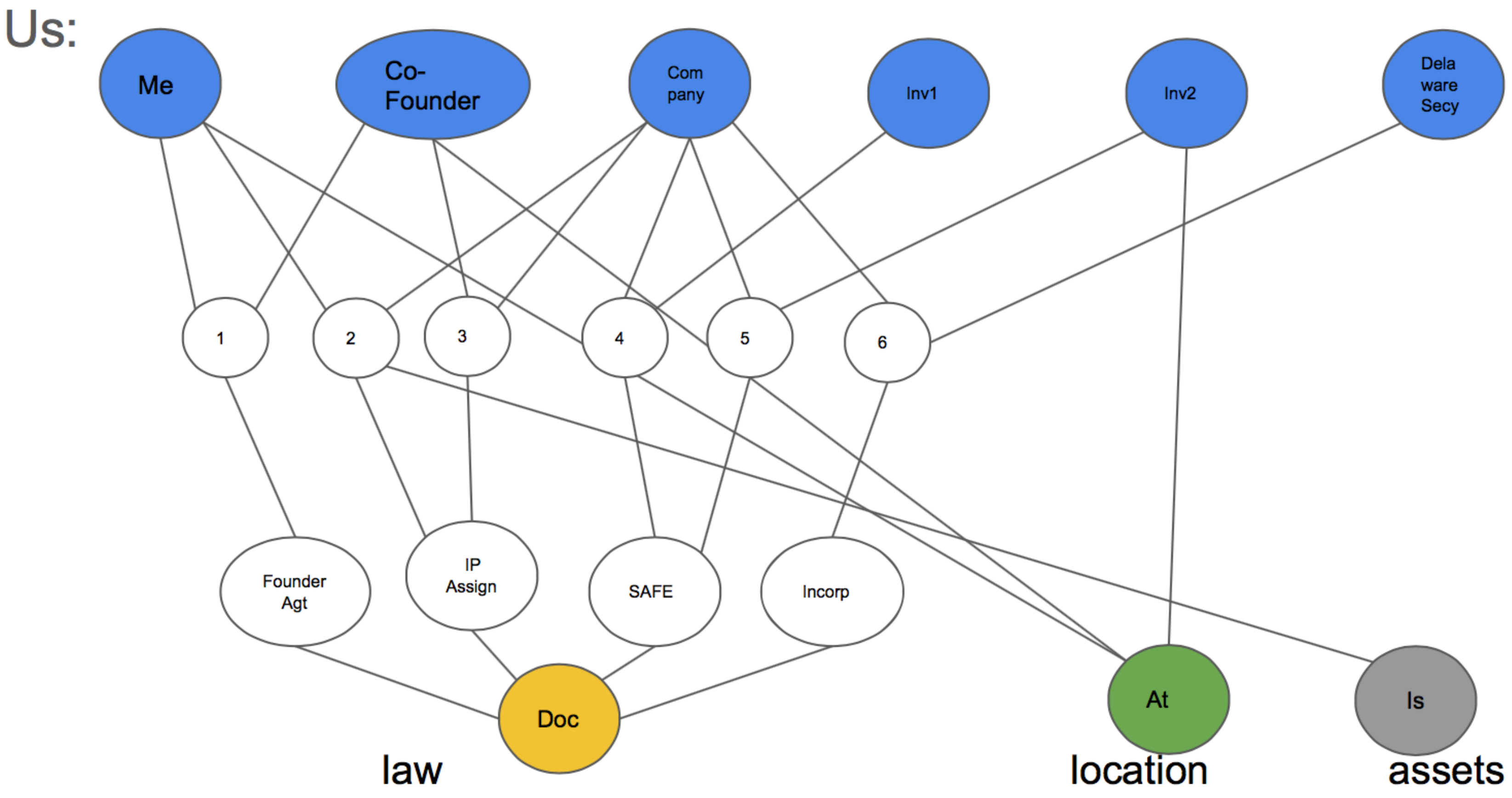
CommonAccord: Model

An object model for a legal system ("graph"):



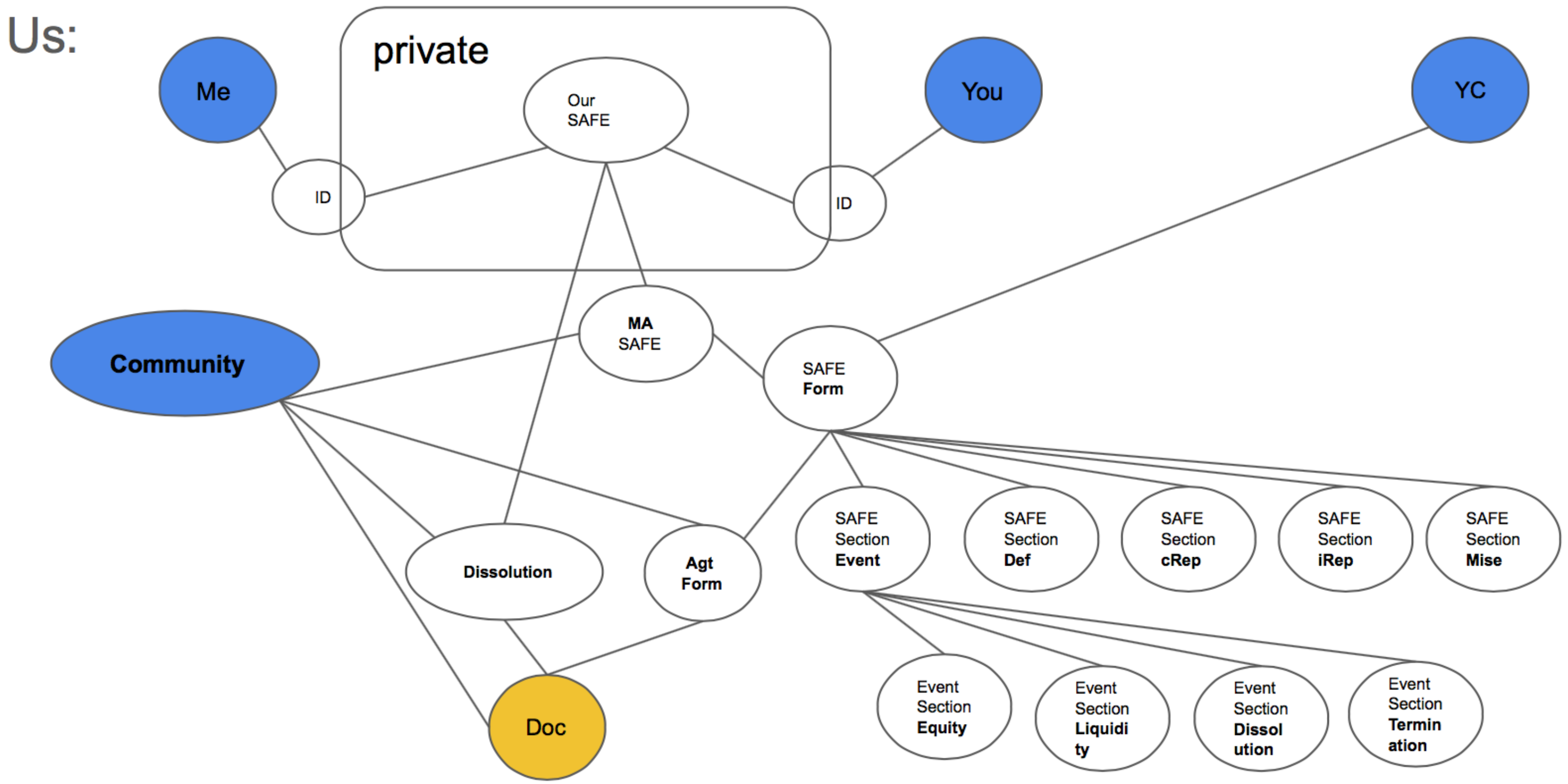
CommonAccord: Model

An object model for a startup financing:



CommonAccord: Model

Object model for a single document:

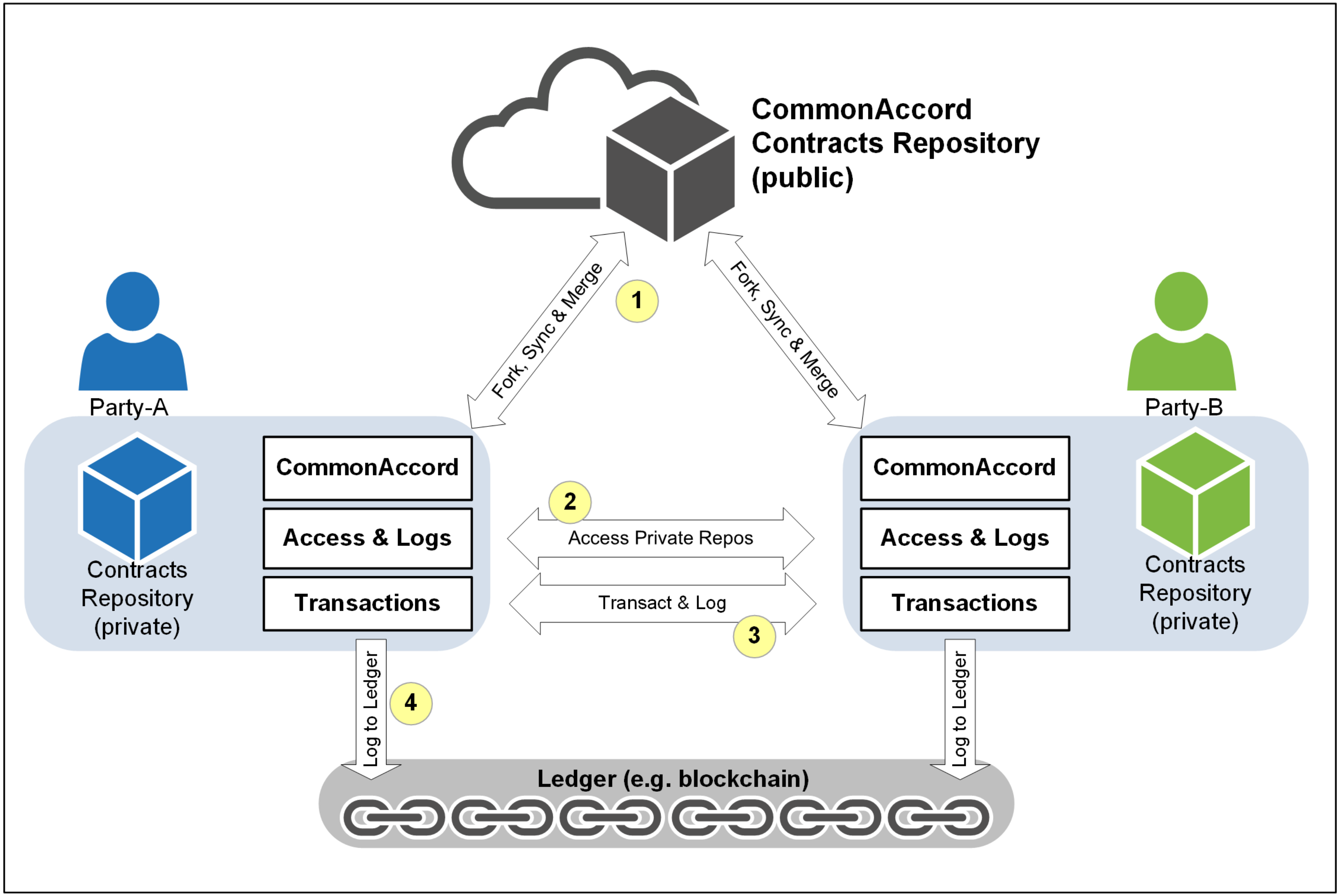


commonaccord.org/i.php?action=source&file=Wx/com/ycombinator/SAFE/Form/Cap_Discount_v01.md

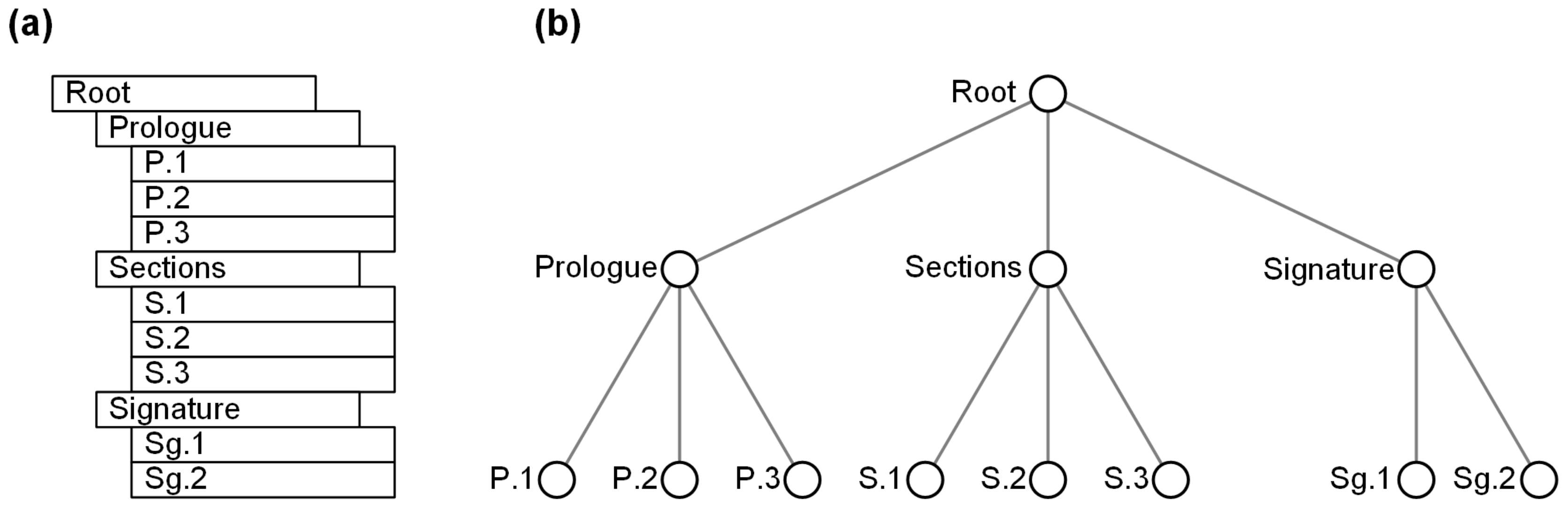
CommonAccord Exchange Network: Architecture

- Data Model and Version Tracking:
  - Data model expresses contracts in modular parts
  - GitHub model for change mgmt & version tracking
  - Parties check-out contract into private repositories
- Access control to contracts and metadata:
  - UMA model for access control to private repositories
  - Parties access repo, do changes, send Metadata
  - Each change generates hash-points in doc hash-tree
- Ledger system:
  - Captures current state of contracts exchange/flow
  - Hash of Metadata added to ledger
  - Can use today’s Blockchain or future technology

CommonAccord Exchange Network



Contract Hash Tree

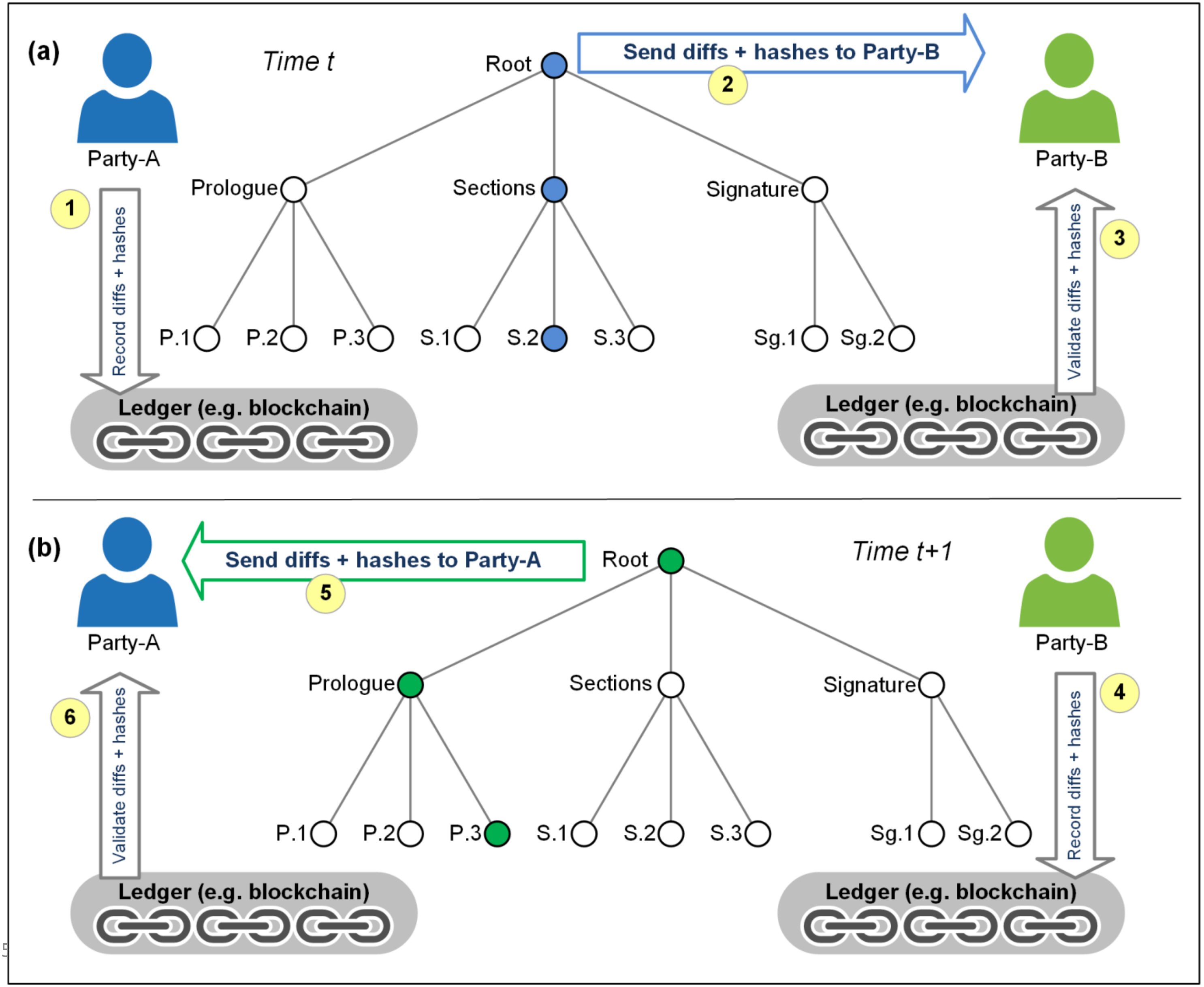


(c)

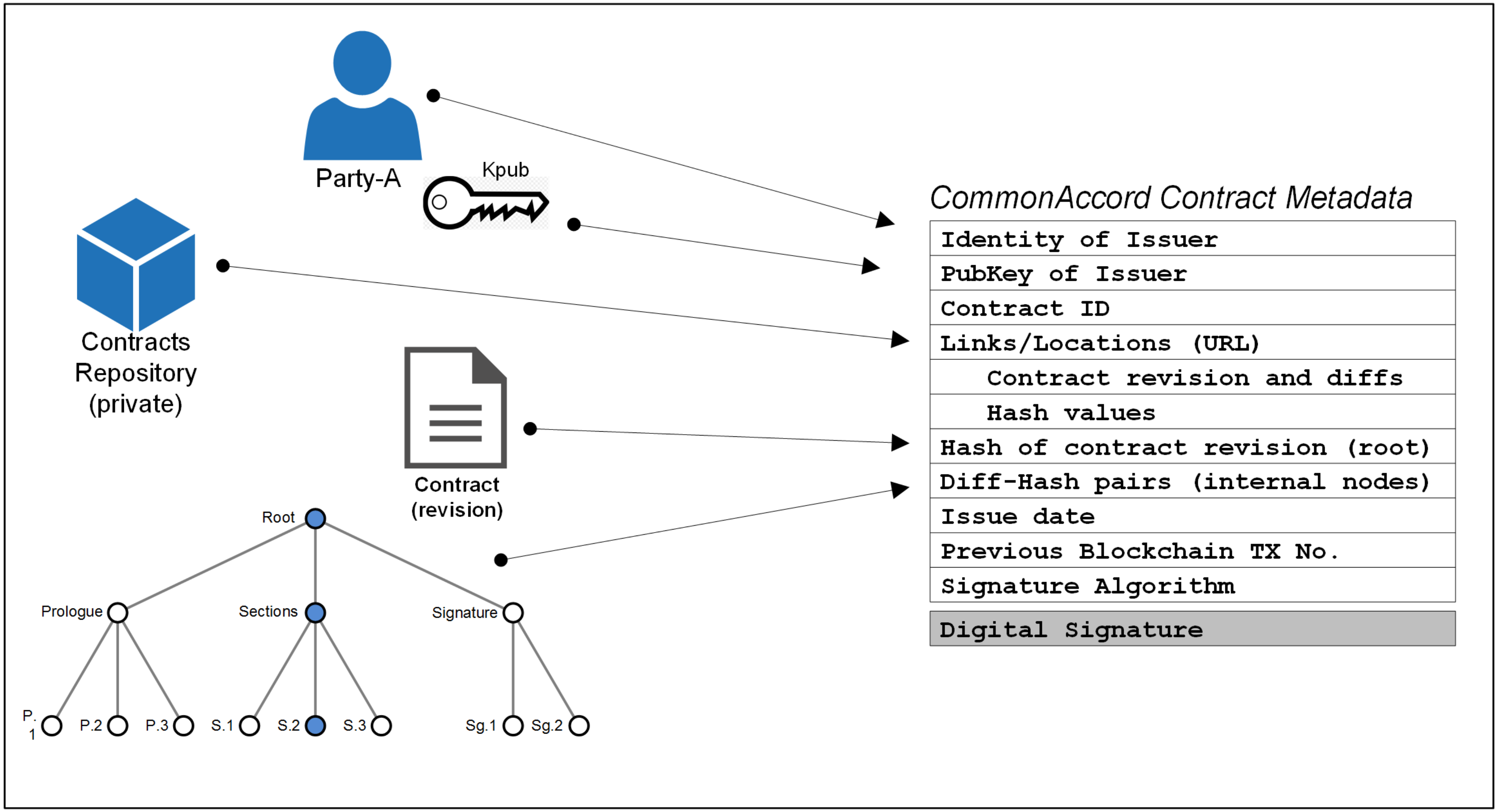
```
Prologue-node = H( H(P.1) || H(P.2) || H(P.3) )
Sections-node = H( H(S.1) || H(S.2) || H(S.3) )
Signatures-node = H( H(Sg.1) || H(Sg.2) )
Root-node = H(Prologue-node || Sections-node || Signatures-node)
```

- Contract expressed as a tree of parts
- Compute hash-points from leaf upwards
- Start contract negotiation using root-document and root-hash
- Contract modification causes new hash-points to be computed

Contract Exchange Flow - Concept



CommonAccord Metadata

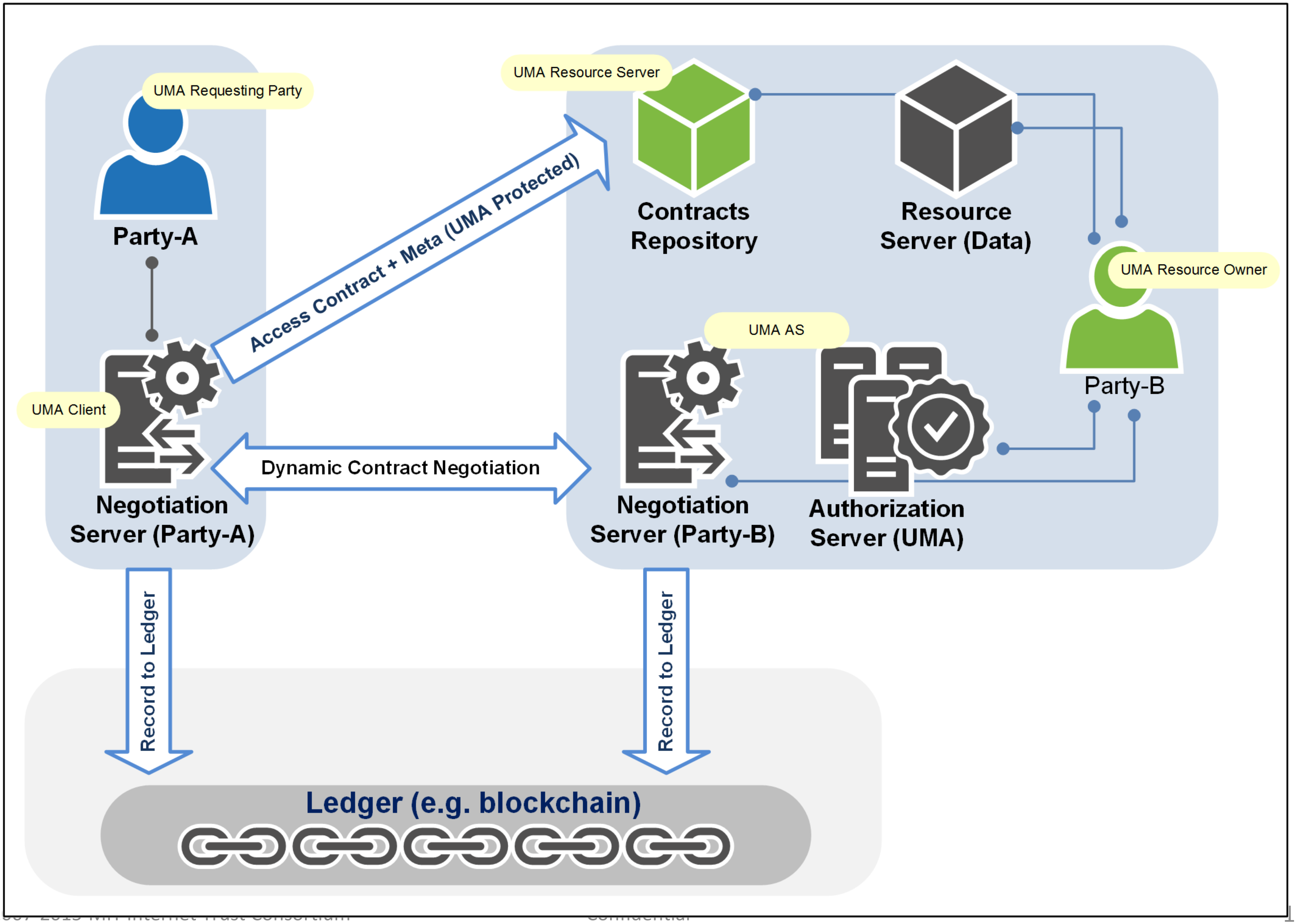


CommonAccord Contract Metadata

```
Identity of Issuer
PubKey of Issuer
Contract ID
Links/Locations (URL)
   Contract revision and diffs
   Hash values
Hash of contract revision (root)
Diff-Hash pairs (internal nodes)
Issue date
Previous Blockchain TX No.
Signature Algorithm
Digital Signature
```

- Metadata captures current state of contract exchange
  - Metadata file sent to (or made accessible in repo to) the negotiating party
- Hash of metadata file recorded onto Ledger

Access Control to Contracts & Metadata - UMA



Possible Future Directions

- Translation of CommonAccord contracts to “executable smart-contracts”
  - Break-up complex contracts into sub-contracts
  - Tree of sub-contracts – contract valid iff entire tree is valid
- Identity Layer
  - Link legal digital identity to blockchain-identity
    - E.g. e-signature X509 certificate
- Supply Chain Contracts Management
  - Combine real-time visibility into state of supply chain
  - Interconnect fulfilment phases to smart-contracts backed by CommonAccord contracts

Thank You & Questions

Thomas Hardjono	[hardjono@media.mit.edu]
James Hazard	[jh@hazardj.com]