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

<table>
<thead>
<tr>
<th>Key</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Doc.Body</td>
<td>{Prologue}</td>
</tr>
<tr>
<td></td>
<td>1. {Agt.Sec.S}</td>
</tr>
<tr>
<td></td>
<td>{Agt.Signature}</td>
</tr>
<tr>
<td></td>
<td>{Agt.Attachment}</td>
</tr>
<tr>
<td>Agt.Sec.S</td>
<td>1. {Sec.Def}</td>
</tr>
<tr>
<td></td>
<td>2. {Sec.Deal}</td>
</tr>
<tr>
<td></td>
<td>3. {Sec.Term}</td>
</tr>
<tr>
<td></td>
<td>4. {Sec.Misc}</td>
</tr>
<tr>
<td>Sec.Misc</td>
<td>{Misc_Title}</td>
</tr>
<tr>
<td></td>
<td>1. {Misc.Notice}</td>
</tr>
<tr>
<td></td>
<td>2. {Misc.Law}</td>
</tr>
<tr>
<td></td>
<td>3. {Misc.Forum}</td>
</tr>
<tr>
<td></td>
<td>4. {Misc.Entire}</td>
</tr>
<tr>
<td>Misc.Law</td>
<td><strong>Law</strong>: This agreement and any dispute relating to it shall be governed by the law of {Dispute.State.the}.</td>
</tr>
<tr>
<td>Misc._Title</td>
<td>Miscellaneous</td>
</tr>
<tr>
<td></td>
<td>1. {Sec.Conf}</td>
</tr>
<tr>
<td></td>
<td>2. {Sec.Use}</td>
</tr>
<tr>
<td></td>
<td>3. {Sec.Care}</td>
</tr>
<tr>
<td></td>
<td>4. {Sec.Compelled}</td>
</tr>
<tr>
<td></td>
<td>5. {Sec.Disclaim.Warranty}</td>
</tr>
<tr>
<td></td>
<td>6. {Sec.Term}</td>
</tr>
<tr>
<td></td>
<td>7. {Sec.Remedy}</td>
</tr>
<tr>
<td></td>
<td>8. {Sec.Notice}</td>
</tr>
<tr>
<td></td>
<td>9. {Sec.Misc}</td>
</tr>
</tbody>
</table>
CommonAccord: Model

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

An object model for a startup financing:

Us:
CommonAccord: Model

Object model for a single document:

Us:

- Me
- You
- YC

- Community
- Doc
- Our SAFE
- MA SAFE
- SAFE Form
- SAFE Section Event
- SAFE Section Def
- SAFE Section cRep
- SAFE Section iRep
- SAFE Section Mise
- SAFE Section Equity
- SAFE Section Liquidity
- SAFE Section Dissolution
- SAFE Section Termination

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

© 2007-2015 MIT Internet Trust Consortium
Confidential
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

1. Fork, Sync & Merge
2. Access Private Repos
3. Transact & Log
4. Log to Ledger

CommonAccord Contracts Repository (public)

Contracts Repository (private)

Access & Logs
Transactions

Party-A

Contracts Repository (private)

Access & Logs
Transactions

Party-B
Contract Hash Tree

- 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

(c) $\text{Prologue-node} = H(H(P.1) | | H(P.2) | | H(P.3))$

$\text{Sections-node} = H(H(S.1) | | H(S.2) | | H(S.3))$

$\text{Signatures-node} = H(H(Sg.1) | | H(Sg.2))$

$\text{Root-node} = H(\text{Prologue-node} | | \text{Sections-node} | | \text{Signatures-node})$
Contract Exchange Flow - Concept

(a) Time $t$

1. Record diffs + hashes
2. Send diffs + hashes to Party-B

Ledger (e.g. blockchain)

(b) Time $t+1$

3. Validate diffs + hashes
4. Record diffs + hashes

5. Send diffs + hashes to Party-A

Ledger (e.g. blockchain)

© 2007-2015 MIT Internet Trust Consortium
CommonAccord Metadata

- 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

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
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]