Digital ID and Shared Ledger Technologies

new models and new ways to work together

Our changing risk landscape

SwissRe Centre for Global Dialogue

November 2017
Identity Impact

Identity is important to the insurance sector (and that’s just for people)

$11 billion up to $17 billion impact
Digital Identity Model

Digital Identity

A simple model to aid discussion
A Three Domain Model

Authorisation Domain  
<table>
<thead>
<tr>
<th>Virtual Identity</th>
</tr>
</thead>
<tbody>
<tr>
<td>dgwbirch! anz.com</td>
</tr>
</tbody>
</table>

Authentication Domain  
<table>
<thead>
<tr>
<th>Digital Identity</th>
</tr>
</thead>
<tbody>
<tr>
<td>dgwbirch!</td>
</tr>
</tbody>
</table>

Identification Domain  
<table>
<thead>
<tr>
<th>Mundane Identity</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dave Birch</td>
</tr>
</tbody>
</table>

from your friends at Consult Hyperion

you want to access this bank account? show me your credentials!
that's the correct credential, how do I know it is yours?
how do I know who you are so I can give you credentials?
Digital Identities

Who creates the Digital ID?

Someone Else

Who uses the Digital ID?

Me
- USB stick

Someone Else
- Only the Digital ID creator
  - government gateway
  - Sovereign Identity
- Others
  - bank card
  - Trans-Sovereign Identity

Self-Sovereign Identity
Customer Authenticates

Customer app needs to digitally-sign response

To do this it needs access to the private key (stored in customer phone)

Customer authenticates to the phone to demonstrate control of the private key

Bank creates a new Read entry in the ledger
Authorisation in the Mass Market

Forget about doing taxes or waiting for banks to come together!

Perhaps internet dating is what we have been waiting for
Understand Shared Ledgers?

What exactly is a "blockchain"
### Shared Ledger Architecture: Layers

<table>
<thead>
<tr>
<th>Layer</th>
<th>Question</th>
<th>Options</th>
</tr>
</thead>
<tbody>
<tr>
<td>Contract</td>
<td>how do we use the transactions?</td>
<td>smart or dumb?</td>
</tr>
<tr>
<td>Consensus</td>
<td>who decides which transactions are valid?</td>
<td>fault or attack?</td>
</tr>
<tr>
<td>Content</td>
<td>what is in the transactions?</td>
<td>data or derivatives?</td>
</tr>
<tr>
<td>Communications</td>
<td>where are the copies of the transactions?</td>
<td>public or private?</td>
</tr>
</tbody>
</table>

Shared ledgers are an innovative combination of new technologies that allow for secure and transparent transactions across various industries. The architecture is structured into layers, each addressing specific aspects of transaction usage, validation, data type, and accessibility.

- **Contract**: Discusses the usage of transactions, distinguishing between smart and dumb approaches.
- **Consensus**: Focuses on who decides which transactions are valid, addressing fault and attack scenarios.
- **Content**: Exploring what is included in the transactions, differentiating between data and derivatives.
- **Communications**: Investigates the location of transaction copies, comparing public and private options.
Shared Ledger Taxonomy

Can anyone use the ledger?
- Yes: anyone can use it
- No: only a selected group

Why do they maintain the integrity?
- Given rewards to the ledger itself
- They are given incentives off the ledger

Who maintains the integrity?
- All group members
- Privileged members

Public Shared Ledgers
- Bitcoin: double permissionless

Private Shared Ledgers
- R3 Quorum: permissioned

Note: The taxonomic distance between ledgers like the Bitcoin blockchain and ledgers like R3.
Shared Ledger Contents

with acknowledgement to Maya Zahavi

What’s in the Blocks?
- data
- hashes of data
- encrypted data
- proofs about data

Why is it in the Blocks?
- global consensus
- time stamping
- coordination within trust group
- auditable privacy

The use of cryptography can deliver new and counterintuitive functionality, and zero-knowledge proofs are a great example of this.

Please copy and distribute
Using a Shared Ledger

Where is the Connection?

How do we connect identity to the blockchain or any other kind of shared ledger?
Identification Domain

We could put “real” identity to the blockchain

you want to access this bank account? show me your credentials!
that’s the correct credential, how do I know it is yours?
how do I know who you are so I can give you credentials?
Authentication Domain

We can put the digital identity (ie, a key pair) on the blockchain (ie, a wallet)
Authorisation Domain

The ledger as an immutable history of proofs about (pseudonymous) virtual identities
What’s Happening?

Blockstack
“decentralised internet”
Sovrin
“self-sovereign identity”
Uport
Shocard
Onenname
BanQu
“economic identity”
BitID
“identity token”
Contact

Visit our website: http://www.chyp.com
Follow us on Twitter: @chyppings
Email us: info@chyp.com
Read: Tomorrow's Transactions Blog
Listen: Consult Hyperion Podcasts

Consult Hyperion UK
Tweed House, 12 The Mount
Guildford, Surrey GU24HN, UK.
+44 1483 301793

Consult Hyperion USA
535 Madison Avenue, 19th Floor
New York, NY 10022, USA.
+1 888 835 6124
Who Are Consult Hyperion?

Consult Hyperion specialises in working out the opportunities and threats which result from the harmony and collision of security, networks and transactions. We are constantly assessing these factors, as they change continuously, and delivering ideas, solutions and products to our clients.
What Do They Do?

We have a structured and practical approach to secure electronic transaction systems from the local to the global

Define
- Strategy
- Roadmapping
- Market Analysis
- Business Modelling

Design
- Prototyping
- Requirements Analysis
- Risk Analysis
- System Architecture

Develop
- Technical Specification
- Procurement Support
- Software Development
- Vendor Management

Deploy
- Project Management
- Certification Management
- Acceptance Testing
- Evaluation

We can help clients in all phases of the product and service lifecycle, from the whiteboard scribble to the person in the street’s everyday use.
Who do we do it for?
Basic Copyright Notice & Disclaimer

©2017 This presentation is copyright protected. All rights reserved. You may download or print out a hard copy for your private or internal use. You are not permitted to create any modifications or derivatives of this presentation without the prior written permission of the copyright owner.

This presentation is for information purposes only and contains non-binding indications. Any opinions or views expressed are of the author and do not necessarily represent those of Swiss Re. Swiss Re makes no warranties or representations as to the accuracy, comprehensiveness, timeliness or suitability of this presentation for a particular purpose. Anyone shall at its own risk interpret and employ this presentation without relying on it in isolation. In no event will Swiss Re be liable for any loss or damages of any kind, including any direct, indirect or consequential damages, arising out of or in connection with the use of this presentation.