Session 6:
Crypto-Assets and Blockchain

Speakers:
Dan Morgan, Ripple
Shermin Voshmgir, Blockchain Hub, Vienna University of Economics
Marc Farag, Basel Committee on Banking Supervision

Moderator:
Aquiles Almansi, The World Bank Group
Things we hear …

• “...an alternative payment system with no government involvement, it has become a combination of a bubble, a Ponzi scheme and an environmental disaster.” Agustín Carstens (BIS)

• “I probably shouldn't say any more about cryptocurrency. But it's not the same as gold or fiat currencies. Those are supported by law, police, courts. ... Blockchain, on the other hand, is real. We're testing it and will use it for a whole lot of things.” Jamie Dimon (JP Morgan)
Digital records

<table>
<thead>
<tr>
<th></th>
<th>A</th>
<th>B</th>
<th>C</th>
<th>D</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Anna</td>
<td>70</td>
<td>45</td>
<td>37</td>
</tr>
<tr>
<td>2</td>
<td>Balances Day 0</td>
<td>70</td>
<td>45</td>
<td>37</td>
</tr>
<tr>
<td>3</td>
<td>Operations Day 0</td>
<td>-20</td>
<td>30</td>
<td>20</td>
</tr>
<tr>
<td>4</td>
<td>Balances Day 1</td>
<td>50</td>
<td>75</td>
<td>57</td>
</tr>
<tr>
<td>5</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Cryptography: hash functions

```
In [1]: import hashlib

In [2]: def hashFunction(string):
   ...:     return hashlib.md5(string.encode()).hexdigest()

In [3]: hashFunction('World Bank')
Out[3]: 'b7b1392937b89054ef8d8bf494c8dae0'

In [4]: hashFunction('World Bank!')
Out[4]: 'd13edd5cfe4bd51de7ec7a25723f6baf'
```
## Hashed Records

<table>
<thead>
<tr>
<th></th>
<th>Anna</th>
<th>Peter</th>
<th>Lucy</th>
<th>Hash</th>
</tr>
</thead>
<tbody>
<tr>
<td>Balances Day 0</td>
<td>70</td>
<td>45</td>
<td>37</td>
<td>'0bb9847ac20152473fd0b0dd55b970b8'</td>
</tr>
<tr>
<td>Operations Day 0</td>
<td>-20</td>
<td>30</td>
<td>20</td>
<td></td>
</tr>
<tr>
<td>Balances Day 1</td>
<td>50</td>
<td>75</td>
<td>57</td>
<td>'bee770c8485eeeeaf7b522555ba6f4ac'</td>
</tr>
</tbody>
</table>
Tamper-Evident Records

Hash of Balances Day 0

```
hashFunction('70,45,37')

'0bb9847ac20152473fd0b0dd55b970b8'
```

Hash of Balances Day 1 = Hash of (Hash of Balances Day 0 + Operations Day 0)

```
hashFunction('0bb9847ac20152473fd0b0dd55b970b8' + '-20,30,20')

'bee770c8485eeeeaf7b522555ba6f4ac'
```
Computer-Network Architectures

Network nodes (yellow) and clients (blue)
Private or Public?

- Private ("permissioned"): all nodes (servers) belong to (are controlled by) the same organization; hence, there is no lack of trust among them.

- Public: anybody can set up a node and join the network; hence, there is zero trust among nodes and it needs a cheating-proof consensus mechanism.
Crypto assets or just records?

<table>
<thead>
<tr>
<th>A</th>
<th>B</th>
<th>C</th>
<th>D</th>
<th>E</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2 Balances Day 0</td>
<td>70</td>
<td>45</td>
<td>37</td>
<td>'0bb9847ac20152473fd0b0dd55b970b8'</td>
</tr>
<tr>
<td>3 Operations Day 0</td>
<td>-20</td>
<td>30</td>
<td>20</td>
<td></td>
</tr>
<tr>
<td>4 Balances Day 1</td>
<td>50</td>
<td>75</td>
<td>57</td>
<td>'bee770c8485eeef7b522555ba6f4ac'</td>
</tr>
</tbody>
</table>
Inside or Outside the Network?

• **Digital assets:** like Bitcoin and other “crypto currencies,” plus assets (and liabilities) created with “smart contracts,” which exist only within (usually public) computer networks.

• **Digital representation of standard assets and contracts:** property registries, contracts such as bonds, bank accounts, derivatives, etc., which exist within a known national jurisdiction.
Our speakers today:

-> Dan Morgan

-> Shermin Voshmgir

-> Marc Farag