

Distributed Autonomous Organizations

Ronald L. Chichester, J.D., CFE, CISA

Presented to the Joint Meeting of
HTCIA and the InfraGuard Tech SIG

January 26, 2017

Houston, Texas

Overview

- The Phenomenon
- The Technology
- More Background
- What's Happening
- What if Something Goes Wrong?



The Phenomenon

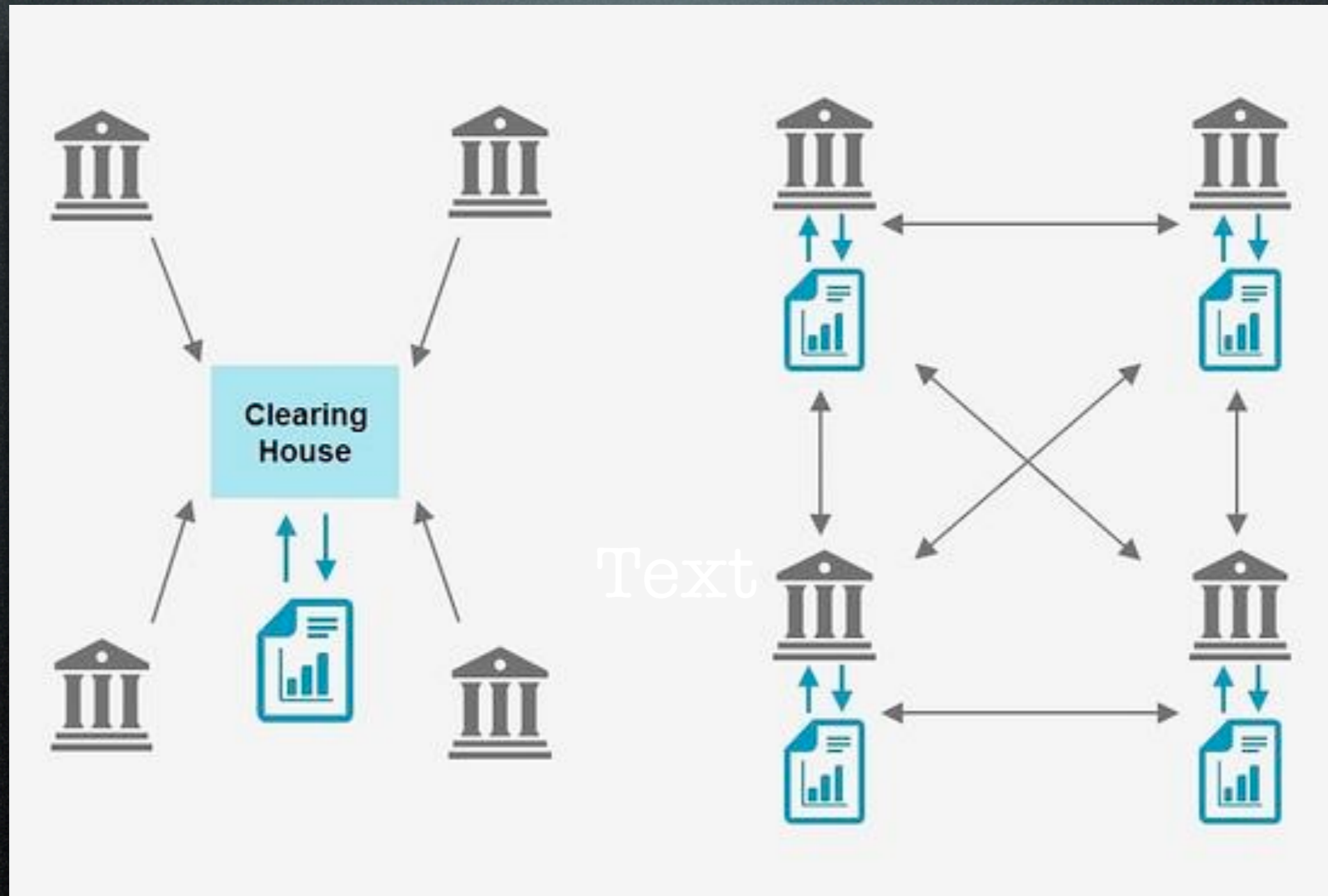


Bitcoin!

The Technology



BLOCKCHAIN



Source: Wall Street Journal

http://online.wsj.com/media/0201_cio_ledg_G_20160201185005.jpg

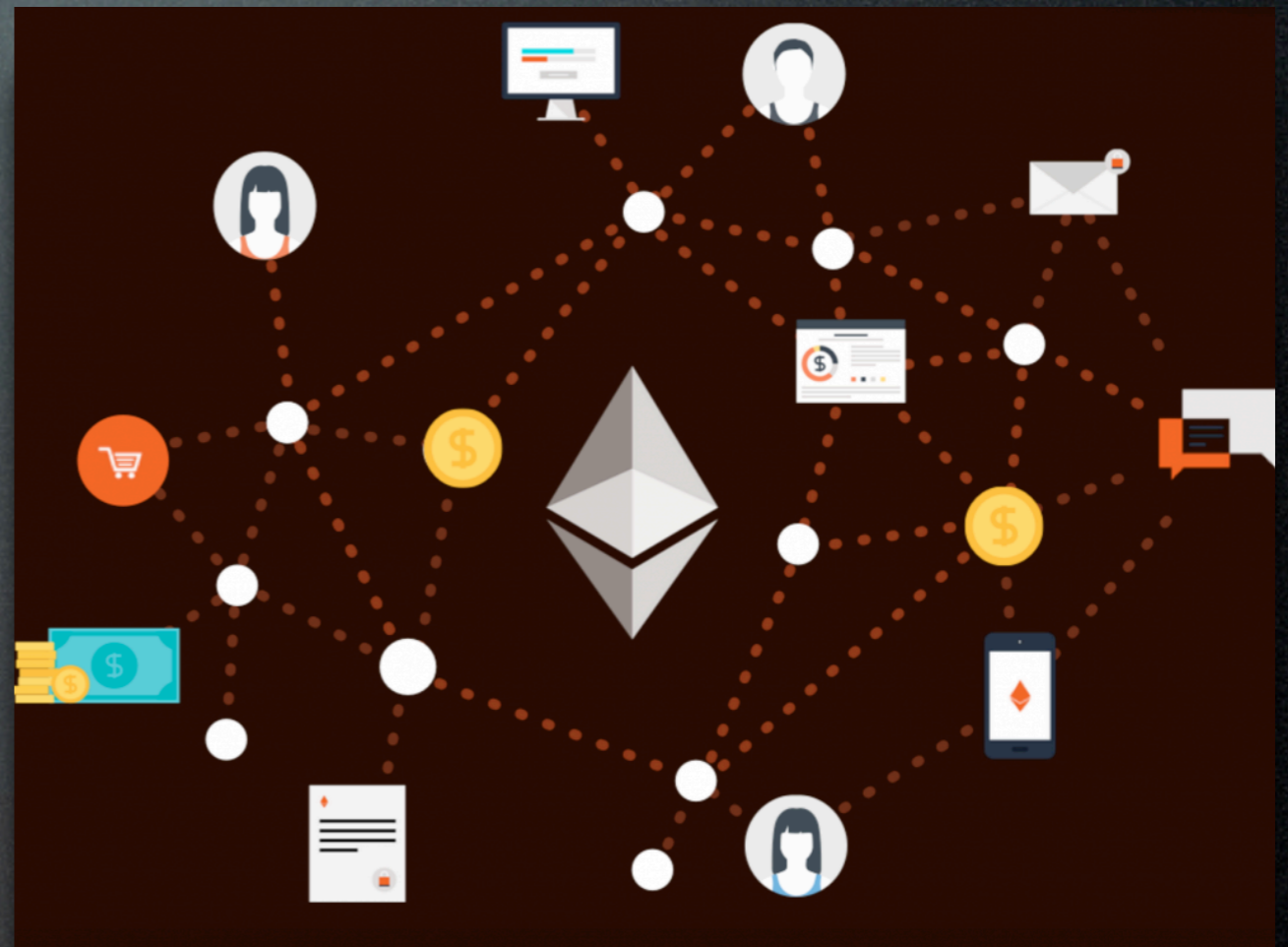
Blockchains

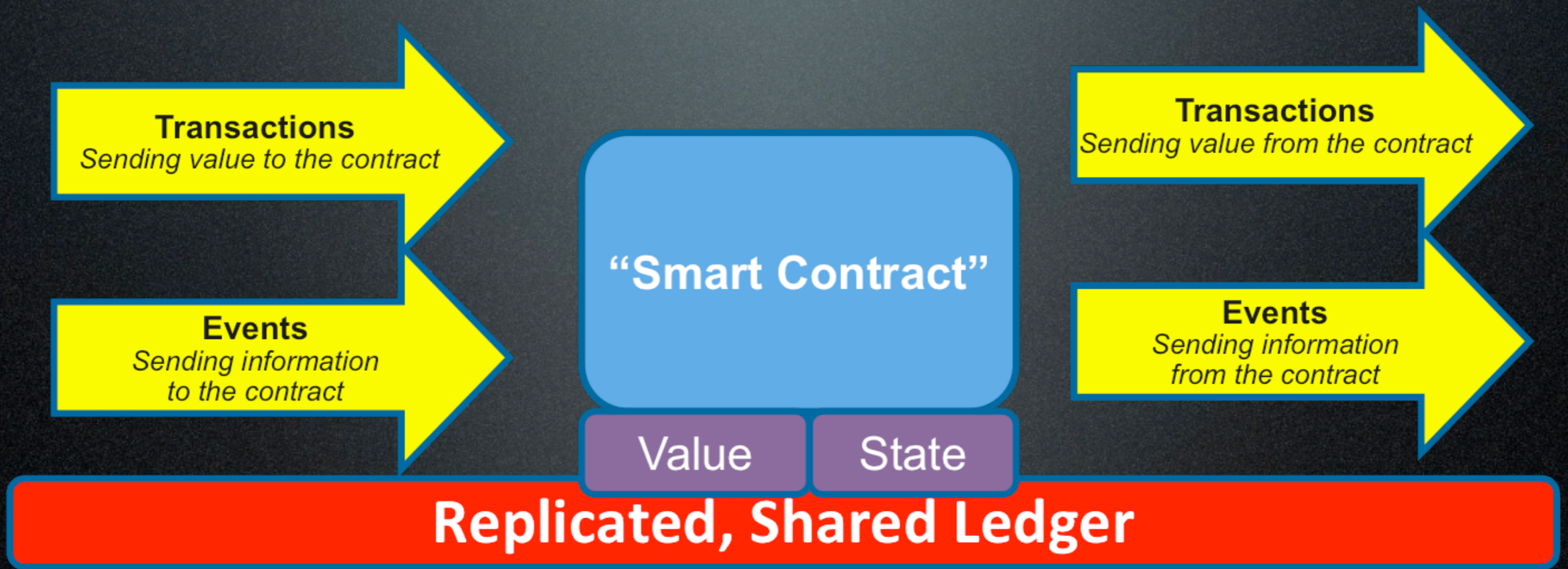
- Record **transactions** ...
- ... in a reliable manner; and
- ... in a manner that precludes refutation of the transaction (by either party)

More Background

Next Steps

- Blockchains are proven
- Can you make an app for that?
- Ethereum, PyThereum, Lisk, StratusPlatform, others...
- Javascript, Python...
- Artificial Intelligence?





Smart Contracts



How OnStar Works

1 GPS satellites orbit the earth at 12,000 miles and continuously stream navigational data



2 The OnStar GPS receiver calculates location data from at least three satellites



3 Upon OnStar button press or automatically in a crash, critical vehicle data is sent via wireless connection



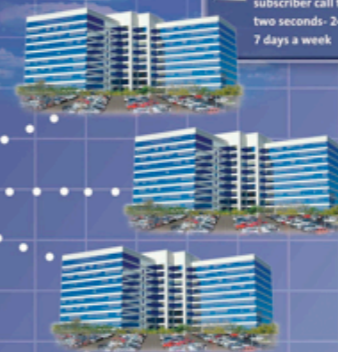
4 Cellular transmission relays calls to the OnStar Data Center



5 The OnStar Data Center receives the call and routes to the appropriate OnStar Call Center and Advisor Group



6 The OnStar Call Centers answer a subscriber call for assistance every two seconds- 24 hours a day, 7 days a week



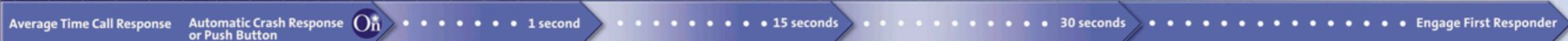
The OnStar Command Center monitors all call traffic, balances volumes between Call Centers and Advisor Groups, and maintains oversight for overall system integrity



7 Trained OnStar Advisors are set up in special teams - such as Emergency or Routing, to better handle subscriber requests. The Advisor desktop application displays street level mapping information with the vehicle pinpointed and Subscriber account information



8 Emergency Advisor contacts Public Safety Answering Point (911) with jurisdiction. Relays pertinent location, crash data and injury status to prepare emergency responders for appropriate rescue strategy

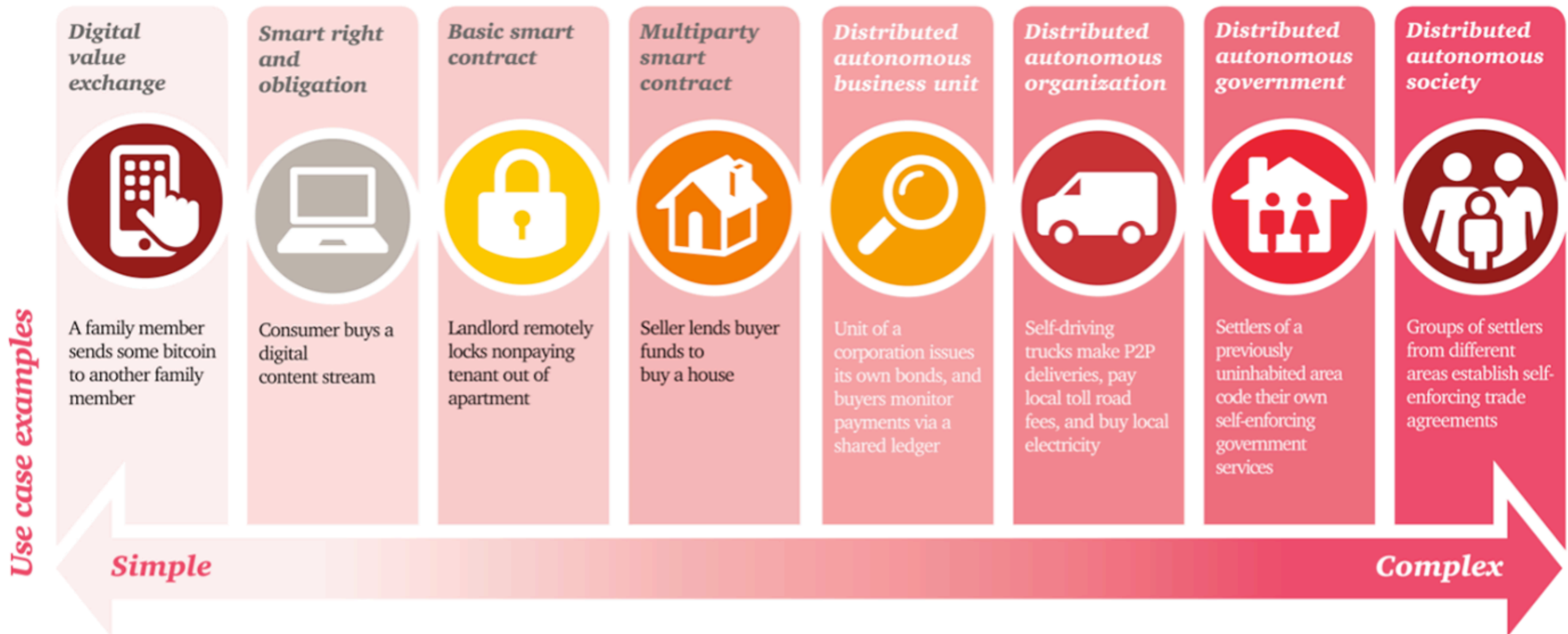


Smart Property



The IoT

Smart contracts – simple to complex



The Spectrum

Distributed Autonomous Organizations

- A corporation in software
- No employees
- No central location
- No need to incorporate

```
pragma solidity ^0.4.0;

/// @title Voting with delegation.
contract Ballot {
    // This declares a new complex type which will
    // be used for variables later.
    // It will represent a single voter.
    struct Voter {
        uint weight; // weight is accumulated by delegation
        bool voted; // if true, that person already voted
        address delegate; // person delegated to
        uint vote; // index of the voted proposal
    }

    // This is a type for a single proposal.
    struct Proposal {
        bytes32 name; // short name (up to 32 bytes)
        uint voteCount; // number of accumulated votes
    }

    address public chairperson;
```

What's Happening



[Download Video as MP4](#)

Rent, sell or share anything - without middlemen

CADE METZ BUSINESS 06.06.16 7:00 AM

SHARE

THE BIGGEST CROWDFUNDING PROJECT EVER — THE DAO — IS KIND OF A MESS



SHARE 18



TWEET



PIN



COMMENT



EMAIL



GET WIRED

Don't Let The Future Leave You Behind. Get 6 Issues For Just \$5.

SUBSCRIBE NOW

MOST POPULAR



CULTURE

Inside the Weird, Industry-Shaking World of Donald Glover

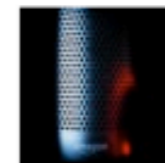
4 HOURS



MOVIES

The New Logan Trailer Plays (Violently) Against Type

1 HOUR

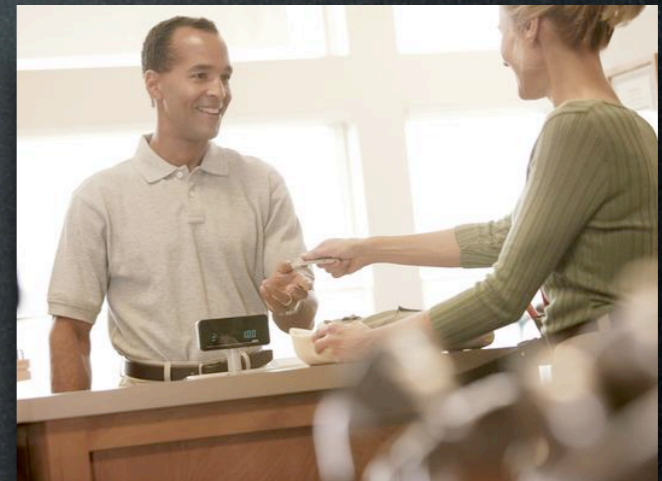


USER INTERFACES

Alexa Is Conquering the World. Now Amazon's Real Challenge Begins

1 DAY

What if something
goes wrong?



Law is the Regulation of
Transactions Among Humans



Redress of Wrongs

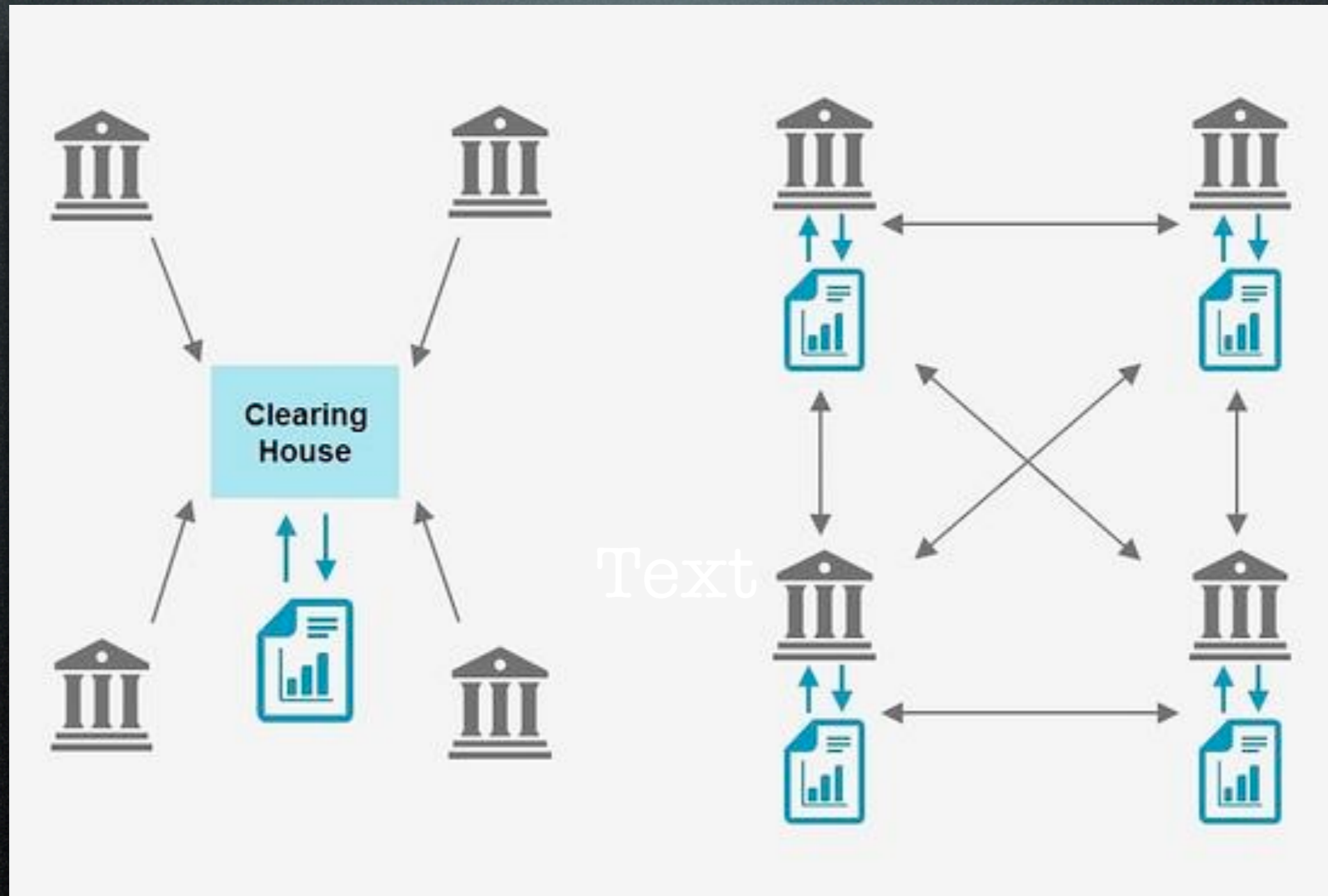
Courts Require

Courts Require Jurisdiction

Jurisdiction

- Jurisdiction comes in two main types:
 - In Personam
 - In Rem





Source: Wall Street Journal

http://online.wsj.com/media/0201_cio_ledg_G_20160201185005.jpg

Problems

- Nodes of the blockchain aren't owned by the defendant
- Nodes can be conducting other lawful activities



Evidence

- Find the nodes...
- Employ a blockchain analyzer...
- Follow the money...
- Find the person...
- Establish **jurisdiction**.



What about encryption?

- Blockchain transactions can be encrypted
- So how can you obtain jurisdiction if you don't know what the transactions are about?
- You don't have to
- That the transactions took place is all you need



Other Interesting Twists

- No persistent storage necessary (but possible)
- Even during function calls
- Have to stop DAO process on ALL nodes before you disable a DAO
- Can't delete previous transactions without breaking blockchain



Other Interesting Twists

- No slack
- No swap files
- Have to discern s/w behavior by piecing together transactions
- Would “sting” transactions be permissible to establish jurisdiction?



Other Interesting Twists

- Code for smart contracts can be compiled from files on multiple (remote) servers
- DAO's can subcontract to other DAO's
- DAO can be given artificial intelligence



Questions?

Ronald L. Chichester

Attorney at Law, CFE, CISA

(713) 302-1679

Ron@TexasComputerLaw.com