Blockchain Series – Part 3 of 4:

How To Build Your First Blockchain App

Please complete a short poll before the session begins: [https://integraleledger.com/poll](https://integraleledger.com/poll)
SPEAKERS

Tori Adams
VP, Government Practice
ConsenSys

David Berger
CTO
Integra Ledger

Peter Buck
VP of Strategy
NetDocuments

Brad Clements
Chief Software Architect
NetDocuments

Stevie Ghiassi
CEO
Legaler
Agenda

• Introduction
• Educational Examples
  – ConsenSys
  – NetDocuments
  – Legaler
  – Integra
• Breakout session/Panel discussion
  – Learn more about the tools discussed
  – Talk through use-cases
• Q & A
CONSENSYS
CONSENSYS

We build blockchain technology and distributed applications that are changing the world.

VISION
Our vision is a world in which distributed applications enable frictionless, efficient, transparent, and accountable government services with inclusion for all.

MISSION
Our mission is to assemble the tools needed to build and scale the emerging economic, social, and political operating system for the planet.
GLOBAL DELIVERY EXPERIENCE

800+ blockchain experts, entrepreneurs, computer scientists, designers, engineers, consultants, and business leaders with delivery experience across 6 continents.
A FULL SERVICE BLOCKCHAIN DELIVERY FIRM

We deliver a full set of blockchain services.

Solutions
Consult and deliver production ready blockchain solutions for organizations and governments

Infrastructure
Help grow the ecosystem by building and maintaining core developer tools and clients

Capital
Provides token services, crypto asset management and venture capital

Products
Incubate new companies developing decentralized applications on the Ethereum blockchain

Education
Educate developers and entrepreneurs about Ethereum through training programs
Ethereum is one of the most powerful social engineering tools developed since the creation of the Internet. Via its ability to create self-executing agreements, tokenized micro-economies, and global, accountable transparent governance systems, Ethereum creates the possibility of developing radically new alternatives to current power relationships and transform existing governmental forms.
ETHEREUM IS ONE OF THE MAJOR BLOCKCHAIN SOLUTIONS

Hyperledger and other blockchain exists – multiple implementations of blockchain exist on the Ethereum ecosystem.

- The Ethereum network processes over **1.1 million transactions per day** (more than all other blockchain platforms combined).
- Truffle, the framework for developing smart contracts on Ethereum has had more than **250,000 downloads**.
  The public Ethereum chain holds roughly **$128bn in value**.
- MetaMask, which uses a plug-in to bring Ethereum seamlessly to today’s browsers, has over **500,000 active users**.
- Infura handles over **2 billion requests** per day and smoothly scaled to peak at 4.5 billion requests per day in December.
- The Enterprise Ethereum Alliance is the largest blockchain consortium
- The Ethereum ecosystem has **30x** the number of developers as other blockchains
BUILDING BLOCKCHAIN
THREE LEVELS OF BLOCKCHAIN QUESTIONS

Working with public and private sector clients, we encounter three distinct levels of blockchain questions.

<table>
<thead>
<tr>
<th>Level</th>
<th>Typical Question</th>
<th>Typical Questioner</th>
<th>Typical Project</th>
<th>ROI/Benefit</th>
</tr>
</thead>
<tbody>
<tr>
<td>Level 1: Blockchain Curious</td>
<td>“Blockchain? That’s Bitcoin right?”</td>
<td>Blockchain Skeptic – typically involved in financial investigations or regulation</td>
<td>Education and Training – “I want to understand blockchain”</td>
<td>Low</td>
</tr>
<tr>
<td>Level 2: Blockchain Enthusiast</td>
<td>“Can you put my existing process on the blockchain?”</td>
<td>Blockchain Enthusiast – found throughout the Federal government</td>
<td>Supply chain POC – “I have a blockchain project”</td>
<td>Low or Medium</td>
</tr>
<tr>
<td>Level 3: Social Engineer</td>
<td>“How can we use blockchain to transform my business?”</td>
<td>Crypto Economics Enthusiast – rarely found in government</td>
<td>Incentive-Based Compliance System – “I have a problem that blockchain might solve”</td>
<td>High</td>
</tr>
</tbody>
</table>

The maximum benefit is achieved by taking risks and solving problems rather than building blockchains.
LEVEL 2: ADVANCE SUPPLY CHAIN PROJECT

Great project but can you achieve this goal by non-blockchain means?

Manufacturer
- Certificate of origin
- Batch numbers
- Processing data
- Shipping data
- Order number
- HSS Code
- Barcode
- Processing data

Distributor
- Certificate of origin
- Batch numbers
- Processing data
- Shipping data
- Order number
- HSS Code
- Barcode
- Temperature

Shippers
- Shipping data
- Order number
- HSS Code
- Equipment number
- Temperature

Warehouse
- Shipping data
- Order number
- HSS Code
- Barcode
- Temperature
- Receive date
- Pickup date
- Packaging specification
- Packaging bar code
- Temperature
- Receive date
- Order number
- Invoice Number
- Customer ID
- Temperature

Pharmacy
- Shipping data
- Order number
- HSS Code
- Barcode
- Temperature

Blockchain
- Records data
- Encrypts
- Layers on-top of and interfaces with existing systems
- Cannot be tampered with
- Visible to Regulators

Smart Contracts
- Match supplier, order, invoice, shipment
- Quality against spec
- Pay supplier (as needed)
LEVEL 3 PROJECT: INCENTIVIZED SUPPLY CHAIN

Great project but could you do it in the federal government?

Each party must pay a fee to join and agree to use a transparent, auditible, high-inspected supply chain. At each stage of the non-purchaser process, an actor (e.g., manufacturer, drop shipper, etc.) purchases a an Ethereum dominated token of sufficient value to disincentivize cheating. If the next party in the process confirms that the package is contraband free, the token is escrowed until the delivery is made. If all parties clear the shipment, the coins are returned to the parties. If a party identifies contraband in a package, then they are given all of the tokens from previous stages. This incentivizes each actor to inspect and verify each shipment. Shippers that lie (i.e., claims problem where no problem exists) would quickly be ejected from the system.

- Certificate of origin
- Batch numbers
- Order number
- Bar code
QUESTIONS TO ASK YOURSELF

When you are building blockchain, ask yourself these questions.

<table>
<thead>
<tr>
<th>Benefit</th>
<th>Relevant to my Problem?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Increased Security</td>
<td></td>
</tr>
<tr>
<td>Increased Transparency</td>
<td></td>
</tr>
<tr>
<td>Increased Auditability and Auditable Record</td>
<td></td>
</tr>
<tr>
<td>Tamper Proof</td>
<td></td>
</tr>
<tr>
<td>Faster Order and Payment Processing</td>
<td></td>
</tr>
<tr>
<td>Greater Trust with Stakeholders</td>
<td></td>
</tr>
<tr>
<td>Incentive Systems System Possible</td>
<td></td>
</tr>
</tbody>
</table>
### HOW DO I START?

Don’t start with a “blockchain problem”, start with a business problem.

<table>
<thead>
<tr>
<th>Identify</th>
<th>Define</th>
<th>Ideate</th>
<th>Prototype</th>
<th>Test</th>
<th>Start</th>
</tr>
</thead>
</table>
| - Work a problem you know and understand:  
  - What’s the problem?  
  - How do you know it is a problem?  
  - Who’s is the problem?  
  - Have you talked to them?  
  - What makes you think blockchain would be a solution?  | - Define the problem or challenge in a single brief statement  
- Validate with stakeholders:  
  - Does this describe your problem?  
  - Have you tried to solve it before?  
  - If so what happened?  
  - Why does it persist?  | - Conduct structure one day workshop  
- Identify personas, epics, and user stories  
- Visualize a radical “to-be” – don’t limit yourself  
- Work to develop a high-impact solution and force yourself to consider if blockchain is the only way to resolve the problem  
- Develop consensus around solution  | - Write a “product review from the future” and get consensus  
- Develop circuit diagram  
- Build paper or software prototype  
- Work with developers and designs – paired programming  
- Expect dead ends and impossible problems  | - Test your solution with stakeholders and people that experience the problem directly  
- Revise as needed  
- Paper or mockups can be good tests  
- Give stakeholders something tangible – it is difficult to imagine something radical that doesn’t exist  | - Finalize your design and begin to create the mechanism to begin to build a POC or pilot  

**This is where the real work begins**
NetDocuments

- Working Definition of Blockchain
- Two Application Examples
INTERNET OF INFORMATION

DEMOCRATIZE CONTENT

CONTENT

Docs
Photos
PDFs
Email
Slides
Web Sites
BLOCKCHAIN = CREATE A TRUE INTERNET OF VALUE

- Money
- Intellectual Property
- Identity
- Deeds
- Contracts
- IOUs
- Insurance
- Property
- Votes

ASSETS

- Energy
- Carbon Credits
- Art
- Books
- Film
- Music
- Votes

Adapted from Don Tapscott
EXAMPLE: PROFILE OF A PURE DIGITAL TRANSACTION

Proof of Work

Identit y

TEXT EXTRACT, INC

CONTOSO LTD

netdocuments
Michael Sanders <msanders@netdocuments.com>

Text Exchange - Addendum 1

To: Michael Sanders

Mike,

Attached is the executed Amendment 1 to the Master Agreement for Text Exchange. Please store and associate with the original agreement.

Thanks,
Chris

---

Attachment: Amendment No 01 to Master Procurement Agreement - TEXT EXCHANGE, INC. and CONTOSO LTD - xx.docx [26 KB]
BLOCKCHAIN ON NETDOCUMENTS

LEGEND

Legal Document

Cloud Content Storage w/URL address

Digital Digest or Finger Print

Blockchain record with time-stamp

PURCHASE AGREEMENT

Secure Link

Document Digest

Blockchain ID

5bae84d2-2876-4645-a3de-752576c33716

https://finalagreement

f5f6726a046265436f66246869737465736469656e746966696361756c756d65

17723398a6351825ac4883f0d25c

566a
BLOCKCHAIN ON NETDOCUMENTS

LEGEND
- W: Legal Document
- nd: Cloud Content Storage w/URL address
- ℓ: Digital Digest or Finger Print
- ℓ256: Blockchain record with time-stamp
ECOSYSTEM
Unlike blockchains that power cryptocurrencies, business blockchains are organized and managed by consortiums or organizations where participants are specified, known, and trusted.
BLOCKCHAIN ELEMENTS IN LEGAL

Standards + Governance

APIs + Permissioned Blockchain

Blockchain Storage
Agreement and Repudiation: How Blockchain Protocols Keep the Heroes and Foes Happy in a Digital Economy.

A Story About Business Blockchains

Peter H. Buck, VP Product Strategy, NetDocuments
Glynna Christian, Partner, Orrick

TL; DR

A blockchain is a tool for a business network. A smart contract is promises compiled into code and stored at a specific blockchain address. Both are useful to business because their efficacy is verified cryptographically.

ABSTRACT

Business and law is encoded in documents, frequently locked in corporate repositories, or unleashed to the world without clear providence. Blockchain is a protocol to allow documents to grant authority for new business events. We call these Business Blockchains.
BLOCKCHAIN FOR PUBLIC KEYS
PROFILE OF ATTACHMENT ENCRYPTION
Home

Favorite Items

- Review of Acme Financials
- Exchange 409 Conflict Bug
- ADV Complying with 'Made in USA' labeling requirements and changes to the California standard
- 16500

To be reviewed

- Trading instructions
- Sales Projections
BUILDING BLOCKS OF NETDOCUMENTS
BLOCKCHAIN EXAMPLES
Proof of Work Example

• Record on blockchain
  – Hash of document content
  – Timestamp
Hash Function

2805DE0274AF9203758 BC9805803203CC823B A29E29...8209
byte[] rawHash = doc.GetContentHash(verNo);
docMetadata.hashAlg = "SHA-256";
docMetadata.source = "ND";
docMetadata.sourceId = "$\{doc.DocumentNumber\}|{verNo}\$";
var queryParams = new Dictionary<string, string>
{
    { "type", DocumentIdentityType },
    { "value", hash },
    { "metadata", JsonConvert.SerializeObject(docMetadata) }
};
string url = BuildUrl("registerIdentity", queryParams);
var response = await CallBlockChain(url);
return response.identityId;
Proof of Work – Verify Document

```javascript
var hashTask = $.Deferred();
DocHash(files[0], hashTask); // start asynchronous computation of the file's hash
var url = 'api/blockchain/id/' + encodeURIComponent(id);
var idTask = $.getJSON(url); // start asynchronous retrieval of the blockchain record
$.when(hashTask.promise(), idTask).done(function (hashResult, idResult) {
    if (!idResult[0].exists)
        status = id + ' is <b>not</b> a document identity registered on the blockchain.';
    else if (hashResult == idResult[0].data[0].value) {
        status = files[0].name + ' is <b>identical</b> to document ' + id + ' registered on the blockchain.';
        status = FormatRecordDetails(status, idResult[0].data[0]);
    } else
        status = files[0].name + ' does <b>not</b> match document ' + id + ' registered on the blockchain.';
    $('#verContResults').html(status);
});
```
Standards Needed for Interoperability

- Format of hash – binary, string (encoding, casing?)
- Indicate hash algorithm used
- Other metadata: source, source ID, ID of creator, ID of creator’s firm, ID of associated matter, digital signature, etc.
using (var cp = new RSACng(2048))
{
    publicKey = cp.ToXmlString(false);
    privateKey = cp.ToXmlString(true);
}
var keyInfo = new BlockchainKeyInfo
{
    keyOwner = (string) dirSvc.UserAttribute("ndEmailAddr"),
    nameSpace =<KeyNameSpace>,
    keyValue = publicKey
};
string url = "$\{KeyBaseUrl\}registerKeyReg";
JObject result = await CallBlockChain(url, JsonConvert.SerializeObject(keyInfo));
Key Standards Needed for Interoperability

• Key encoding – W3C XML, .NET XML, PEM, hex-encoded binary DER
• Key algorithm – RSA, ECC
• Key length
• Key revocation
Identity Standards Needed for Interoperability

• Form of identifier – email address, name, passport number, etc.
• Identity verification
• Namespace coordination
Encrypted Email Example – Encrypt Attachment

```csharp
private byte[] GetHeader(SymmetricAlgorithm symCrypto, string originalExtension)
{
    // Header format: 4 byte alg identifier, 8 byte original file extension, 4 byte IV length, 4 byte encrypted key length, IV, encrypted key
    // Note that for AES the IV length is the same as the block length.
    // The size of the encrypted key will match the size of the asymmetric key.
    string prefix = "$\{\text{Alg1}\}\{\text{originalExtension.PadRight(8, ' ')}\}\{\text{symCrypto.BlockSize.ToString("D4")}\}\{\text{mAsymmetricProvider.KeySize.ToString("D4")}\}"
    byte[] header = new byte[prefix.Length + symCrypto.BlockSize / 8 + mAsymmetricProvider.KeySize / 8];
    Encoding.ASCII.GetBytes(prefix, 0, prefix.Length, header, 0);
    symCrypto.IV.CopyTo(header, prefix.Length);
    var encryptedKey = mAsymmetricProvider.Encrypt(symCrypto.Key, RSAEncryptionPadding.Pkcs1);
    encryptedKey.CopyTo(header, prefix.Length + symCrypto.BlockSize / 8);
    return header;
}
```
Encryption Standards Needed for Interoperability

• Sender must communicate to recipient:
  – Symmetric encryption algorithm and key length
  – Encryption algorithm parameters (padding mode, block length, etc.)
  – Initialization vector
  – Encrypted symmetric key
  – Original file extension
A DIGITAL LEDGER TO THE INTERNET

**TIME**

**FEATURES**

A blockchain needs two things: data and data in sequence known as blocks. The data is digitally digested or hashed, then chained together into blocks using time stamps and cryptography. The Time Stamp creates order.

**DIGITAL**

**FEATURES**

Certainty is created through a digital digest of a document. While a hash looks like a bunch of random numbers, it is invaluable because it uniquely identifies the document. The hash gives every document a "digital fingerprint." Every hash is a fixed length; the same data always produces the same result. Hash is practical because it is easy to compute yet infeasible to convert back to data.

**DISTRIBUTED**

**FEATURES**

Blockchains are a network of distributed computers, connected using software protocol. The union of a software protocol and a distributed database is blockchain.

Blockchains enable trust through transparency. A shared distributed ledger is visible only to participating organizations. Business Blockchains are a viable solution when many parties need to access, create and maintain records over an extended timeframe.

**LINKED LIST +**

**FEATURES**

Linking or “chaining” each contribution to a blockchain by hashing the block contents, creates an immutable sequence much like a DNA string. Building and maintaining these lists is expensive and tokens create an incentive mechanism for participation. Markets for these tokens can be created to store value, e.g., BitCoin, or currency.
# THE BLOCKCHAIN JOURNEY

<table>
<thead>
<tr>
<th></th>
<th>Internet in 1994</th>
<th>Cryptocurrency in 2017</th>
</tr>
</thead>
<tbody>
<tr>
<td>Global Adoption (Users As % Of Population)</td>
<td>0.25%(^1)</td>
<td>0.5%(^2)</td>
</tr>
<tr>
<td>Single Current Use Case w/Major Traction</td>
<td>Email</td>
<td>Bitcoin (&quot;swiss bank in your pocket&quot;)</td>
</tr>
<tr>
<td>Functional Use Cases W/Early Traction</td>
<td>Journalism, Personal Blogs</td>
<td>Anonymous Transactions, Crowdfunding</td>
</tr>
<tr>
<td>Use Cases That Are &quot;Too Early&quot;</td>
<td>Online Retail, Streaming Video</td>
<td>Most Decentralized Applications</td>
</tr>
</tbody>
</table>
LEGALER
The Blockchain Infrastructure for the Future of Legal Services
The Legaler Infrastructure

**LEGALER DAPPS**
An ecosystem of dApps to reinvent legal services and enable access to justice by eliminating intermediaries. Legaler Foundation will help facilitate funding for future projects proposed by the community.

**LEGALER BLOCKCHAIN**
A privacy-preserving blockchain specialised for the legal industry. Economical, scalable and interoperable with major legal platforms and protocols, including OpenLaw, Clause.io, Ergo, Accord Project and more.

**LEGALER PLATFORM**
Developer libraries and protocols to easily build dApps using an SDK and API. The Legaler open-source protocols define functionality standards for identity, payments, transaction stages, communication and dispute resolution.

**LEGALER DAO**
Legaler will progress towards a fully Decentralised Autonomous Organisation (DAO) to govern the Legaler infrastructure and support the ecosystem of dApps through token incentivisation.
**Legaler Blockchain**

The Legaler Blockchain has been designed for the strict confidentiality requirements of the legal industry and as a solution to existing scalability limitations of public blockchains.

**SCALABLE**
Randomised Delegated Proof of Stake (RDPoS) consensus algorithm delivers instant finality with the potential for millions of nodes.

**SECURE**
Practical Byzantine Fault Tolerance (PBFT) ensures consensus can be reached in the event of significant malicious attacks on the network.

**ECONOMICAL**
Industry specific blockchain allows for significantly cheaper transaction costs through increased performance and less competition.

**PRIVACY**
Zero-Knowledge Proofs allow for privacy-preserving transactions and client-side encryption secures all stored data in transit and at rest.
Legaler Platform SDK

Legaler Platform SDK gives businesses and developers the power to reinvent legal services by building middleman-free marketplaces, recruitment and referral networks, crowd-sourced litigation funds and more. The possibilities are endless.

Legaler Protocols

- **IDENTITY**
- **COMMUNICATION**
- **TRANSACTION**
- **PAYMENT**
- **DISPUTES**
Legaler Aid
The World’s First Decentralised and Self-sustaining Legal Charity.

**FOR CLIENTS**
Access to free legal services through donations and pro bono lawyers

**FOR LAWYERS**
Discover hidden work in areas of interest while earning revenue

**FOR DONORS**
Monitor every contributed dollar from donation to outcome

**FOR LEGAL CENTRES**
Connect with funding and pro bono lawyers eager to help
What are you going to build?

Get in touch

stevie@legaler.com
@legalerhq
<table>
<thead>
<tr>
<th>Easy but Limited</th>
<th>Difficult but Enterprise</th>
</tr>
</thead>
<tbody>
<tr>
<td>Integra Ledger with Postman</td>
<td>Integra Ledger with RESTful SDK from Web App or Service</td>
</tr>
<tr>
<td>Hyperledger Fabric With Playground</td>
<td>Hyperledger Fabric With Composer and Dockerized Development Environment</td>
</tr>
<tr>
<td>Zapier</td>
<td>Truffle with Ganache</td>
</tr>
<tr>
<td>Udemy Select course on Ethereum or Hyperledger</td>
<td>Azure or AWS Blockchains</td>
</tr>
<tr>
<td></td>
<td><a href="https://media.consensys.net/everything-you-possibly-need-to-develop-on-ethereum-1bef0c23c7c6">https://media.consensys.net/everything-you-possibly-need-to-develop-on-ethereum-1bef0c23c7c6</a></td>
</tr>
</tbody>
</table>
Integra Ledger API

- RESTful API
- 5 Endpoints
  - registerIdentity
  - identityExists
  - valueExists
  - regKeyReg
  - keyRegForOwner
API Access

All calls to the ledger must include the following header:

- Content_Type : application/json
- Authorization : Bearer xxx

Please contact dberger@integraledger to obtain a development token.
POSTMAN

https://www.getpostman.com/
TRUFFLE

https://truffleframework.com/
BREAKOUT SESSIONS
QUESTIONS TO CONSIDER DURING BREAKOUT SESSION

• What problem are you trying to solve, or what opportunity are you trying to pursue?
• Why is blockchain an appropriate tool for this use case?
• Which flavor of blockchain did you pick? Why?
• What development tools and skills will you need?
• What integration will be required with other software tools?
• How will you accomplish those integrations?
• What technical obstacles, or speed bumps, do you see on the road to completion of your project?
QUESTIONS?