Blockchain, Identity, Trust & Governance
BITGov Workshops

Workshop Report: Considerations from the Inaugural OIX Blockchain, Identity, Trust and Governance Workshop

The Future of Distributed Ledger Technology and Legal Frameworks

Contents

Introduction

As more and more applications and use cases are coming closer to market on distributed ledger technologies, such as blockchain, we see both the massive potential this technology can deliver, as well as the looming challenges in guaranteeing their fairness and trustworthiness. This is where the intersection of IT and legal expertise will be critical. The convergence of these disciplines is going to be fundamental for developing the governance frameworks and trust mechanisms necessary to propel the success of distributed ledger initiatives including, but certainly not limited to: cryptocurrency distribution, self-sovereign identity management, public and private voting mechanisms; and smart contracts, both from societal as well as regulatory standpoints.

The Open Identity Exchange (OIX), with support from the Distributed Ledger Foundation (DLF), recognizes the significant impact that thought leaders around the world – whether technical, legal, or legislative – can have in providing guidance for the governance frameworks that will serve these applications, the businesses or organizations deploying them; and the people who will depend on them. This recognition led to the organization of the OIX Blockchain, Identity, Trust and Governance (BITGov) Workshop series.

These workshops are one-day educational workshops for lawyers, policy makers, and technologists involved in deploying systems at scale utilizing blockchain and distributed ledger technology. The goal is for participants to share their expertise and create a global community dedicated to interdisciplinary knowledge exchange, and the formation of best practices that will inform private enterprises, public entities, and governmental bodies on how to responsibly and successfully deploy projects using distributed ledger technology. This paper provides insight into the discussions and debates that have been held through these workshops.

Don Thibeau

Chairman & President, Open Identity Exchange

Chairman & President, Distributed Ledger Foundation

The Current State of Blockchain, Law and Governance

We are currently at a critical juncture in the development of smart legal contracts that places us at the cusp of seeing the widespread adoption of these instruments for complex commercial transactions. Due to this, the importance of building trust into the systems that will support them at this early stage is high. There is potential for distributed ledger technology (DLT) to be embraced by most of the commercial world to do just that, as long as the technology can adequately protect against risk and uncertainty. In order for this to happen, DLT must be accepted as trustworthy for each specific application and use case, regardless of which industry it relates to – and beyond establishing at simply a technical level that a particular system works reliably.

This means determining appropriate professional gatekeepers who are able to exercise their experience and judgment to determine what the parties to these smart contracts will need to have programmed into these agreements, and what needs to be done to comply with existing legal structures.

> **A close collaboration between technologists and these professional gatekeepers is crucial at this early stage so that they can collaboratively design these systems with the necessary protections and legal considerations baked into the technology itself.**

To gain an understanding of where market forces will drive us, we should look at the two commercial functions that DLT can accomplish within the context of smart contracts: executing transactions; and record-keeping and transaction monitoring.

Executing Transactions

Looking at DLT from the perspective of the cryptocurrency use case, attention is placed on the technology as a means of distributing the confirmation of transactions. Today, the focus is on looking for the efficiencies and speed that can be gained from the use of a distributed ledger in the confirmation process.

> **This view may be short-sighted and misses the greater benefit of DLTs, which is that they can also support stronger, more secure, and more trustworthy interactions.**

This is not dissimilar to the early years of the internet where initial expectations were that transactions on the internet were going to take place outside of existing legal systems, and therefore would never work for large scale, mainstream applications. There were expectations of disintermediation – where stocks could be traded, commercial loans secured, Ferrari ownership transferred from one party to another – all without worrying about things like government regulation, broker deal regulation, etc. Those expectations were unfounded.

> **Instead what happened was that the legal systems and regulators had to adapt themselves to permit businesses and individuals who demanded being able to use the internet to transact to do so faster, more easily, and more efficiently.**

In the transfer of money for assets, we must understand that, at the point of actual transaction, the current “real world” system relies on lawyers, accountants, and other oracle gatekeepers to exercise judgement, and to give parties assurance as to whether the transaction should be completed. There are all sorts of legal issues in the real world that will burden whether a transaction can be completed. There are subtle expectations of commercial parties that have existed for centuries and are embedded in legal systems of every jurisdiction. And there are agreements which parties expect to be able to make for what they will do after the transaction closes, and what will happen if things go wrong.

> **This will not go away, and all parties to a contract rely on these being represented and incorporated in any transaction they do.**

In the use case of smart contracts, there is a relationship between human prose of a traditional contract and code used to script these agreements. Some approaches to structuring smart contracts include completely replacing traditional (paper) contracts with smart contracts (computer code). Alternatively, a hybrid approach combines aspects of traditional contracts with smart contracts. The latter often involves bifurcating contracts into two parts; self-executing code and human prose. The human prose element (e.g. an arbitration clause) would remain in traditional from, while the self-executing element (e.g. the transfer of a cryptocurrency, such as bitcoin or ether, between two parties) executed, in code, on a blockchain.

An example would be a smart contract that is used to transfer the ownership of a Ferrari from one party to another. Here, the transfer of payment could occur automatically (via code) - upon the smart contract's receipt of notice (from, perhaps, the Department of Motor Vehicles), this would trigger the transfer of ether from one party to another. However, the purchasing party may want to bargain for certain representations and/or warranties with respect to the vehicle. These provisions (e.g. a representation that the vehicle's manufacturer's warranty is in good standing) may be better addressed in the form of a traditional contract.

> **We are likely to see hybrid approaches combining law-blockchain. For example, a human-language contract will be signed and identically reflected on the blockchain, with some automated aspects on blockchain. Soft details that people "expect" from legal contracts can then be built in.**

Record Keeping and Transaction Monitoring

The crucial "smartness" of DLT, for current purposes, is that it provides a uniform base of information - a single source of data - on which all parties to a transaction can rely for evidence of the details of that transaction. In some derivatives markets, where trillions of dollars in transactions are generated each day, the participants are all entering the transactions into their own systems. This introduces tremendous potential for error. The elimination of reconciliation efforts in these markets could reduce transaction costs by billions of dollars every year.

> **DLT permits us to expect a reduction of input errors, and the time it takes each participant to verify whether a party has the claimed rights. The increased accuracy of records across markets will lead to a significant reduction in disputes and needless litigation.**

This will only succeed to the extent that we gain market acceptance. Participants must be able to rely on DLT to replace existing formats upon which they are already comfortable relying.

> **For this, there needs to be a focus on building ties with existing systems; with mediators and gatekeepers on whose trust existing systems function.**

Engineering Legal Solutions

A current perception of the use of DLT as a means of deploying applications that are intended to facilitate trusted transactions at internet scale is that it can seem chaotic and full of risk. This perception must be dispelled through collaboration between the technical and legal communities, so as to bring order to this perceived disorder. First steps to doing so require the following questions to be considered:

- *What is the nature of the risk we have now?*
- *What might blockchain help us do?*
- *What are the ways in which these instruments can be de-risked?*

It has been observed that where the instruments we trade do not have a physical element to them, it is hard for people to embrace new models of thinking and operating with regard to these assets.

> **A way to lend tangibility to these ideas is to think of taking the intangible rights of people and put them into distinct, separate components to make them quantifiable and portable. These components can then be moved around, sold, bought, and consumed.**

Given the new set of risks emerging from greater consideration of DLT as a means of supporting legal agreements at internet scale, how much can blockchain help to compartmentalize new and aggregated old risks, in order to commodify, normalize, and regularize any intangibles?

Humans tend to project out externalities through forming the narrative of deities, countries, companies etc. These abstractions bound by a framework of rules allow for predictable future human-to-human interactions. The blockchain offers another enforceable narrative, normalizing and de-risking future interactions. These rule-bound narratives outlive individuals. They are sustained intergenerationally by the abstracted organizations.

The perpetual nature of storage on blockchain means it maintains a signal through time. This has incredible potential value. So how can we commodify that value and compartmentalize it in order to make it portable, trade in it, divide it, etc?

> **The more abstracted and normalized an asset, the easier the standardizing of transactions - the easier it is to mechanize its transfer.**

What is the nature of the risk we have now? How can a nuclear network with a distributed architecture resist the failure of network participants, i.e. nodes? All human organizations are hierarchical information flows: governments, companies, NGOs, co-ops. They engage in hierarchical decision-making.

> **Hierarchies depend on centralized decision flows. Decentralized systems with no central control have no central lever point.**

When one is asked who they are, they cite externalities - abstractions - where they went to school, where they work. These are standardized units of identity. Blockchain - and the decentralization of systems, which is an integral part of it - comes with the possibility of institutional failure. It is an existential moment for our centralized, institutional brokers of trust. Current institutions are losing their identity and their ability to control. We need newer, smarter methods to attract people to modern institutions.

Two use cases of blockchain that are growing at an explosive rate are cryptocurrency and personal data management – i.e. storage, extraction, and exploitation. Each of these two use cases is growing without any sufficient legal framework. It has been suggested that this is partially intentional - a reflection of the libertarian, anarchic thinking of “ask forgiveness, not permission”. The result, if this continues, is a legal train wreck waiting to happen.

> **The two big issues where greater exploration is needed are*:* the legal status of a blockchain; and, ensuring the security of personal data.**

What is the Legal Status of a Blockchain? Is a Blockchain a Partnership?

It is inevitable that there will be a disagreement between parties to a transaction in how a contract is executed. When this happens, the plaintiff class-action bar will argue that it is a statutory partnership:

> UPA SS 202(A): “the associations of two or more persons to carry on as co-owners of a business for profit forms a partnership, *whether or not the persons intend to form a partnership*.”

While this is not the necessary result, it is a possible one, and it is the main line of attack from traditional fiat interests. This would be a disaster for those active in the chain, including nodes and miners. A default “partnership” scenario, would mean joint liability for all “partners”; governance issues and fiduciary duties, whereby every “partner” has an equal vote (e.g. not through mining power); and potential tax implications, whereby there may be US taxation on all “partners”, worldwide.

> **Default partnership rules, if applied to blockchain entities, would be catastrophic.**

One proposed solution is a Blockchain LLC. This proposal is already pending in Vermont Bill (S269). This would mean:

- Electing this subcategory of LLC
- A limited liability shield
- The technology can be the operating agreement, whereby some form of consensus algorithm is set
- Authorizing governance on forks and changes
- Participants could also act for their own account, and in geographic isolation
- A Sub-C taxation election could be layered on for international treatment, meaning that non-US citizens do not have to pay US taxes.

Governance topics include defining and specifying rules around:

- The type and purpose of the ledger - whether it is a public or private chain, and how decentralized it is
- Adopting and changing the consensus algorithms, and how to push software updates
- Fixing breaches (e.g. rules around forks by vigilantes)
- Membership: categories, duties, rights, limits on fiduciary duties

The next step, then, would be to define the Operating Agreement.

How Do We Protect Personal Data?

The issue of exploitation of personal data is already significant - it already affects consumers. There is massive exploitation of our data. European regulators are moving to restrict this exploitation, whilst private solutions like OIX may also be possible, and are more in keeping with the US ethos. A personal information protection company is a business organized for the primary purpose of providing personal information protection services to individual consumers.

> **Identity management as a business goes a step beyond OIX to include legal metadata on personal identity management (e.g. the fiduciary duty for the companies).**

"A personal information protection company that accepts personal information pursuant to a written agreement to provide personal information protection services has a fiduciary responsibility to the consumer when providing personal protection services."

> **Here, the company's fiduciary duty is baked into their charter, most notably the notion that the company *has* to be responsible to the consumer. This would be a signal of trust and would set best practices going forward.**

We are heading towards some serious legal failures with regard to currencies and personal data on blockchain.

> **These hot areas of technology will benefit from having appropriate legal framing available - not just regulatory, but also recognized legal structures. These legal framings need to be developed at the State-level for greater integrity.**

Multi-Party System Governance and the Shared Signals Use-Case

Examples of multi-party systems include:

- Credit card systems, e.g. American Express, Discover, Mastercard, Visa
- Payment systems, e.g. ACH, SWIFT, ATM systems
- Identity systems, e.g. SAFE-BioPharma (pharma sector), InCommon (education sector), Gov.UK Verify (UK residents), eIDAS (EU residents)

There can be thousands of participants, or millions, in a credit card system. There can be a common transaction type or set of types (e.g. API). And there can be random (unspecified) interactions among participants, where anyone can interact with anyone in the system. For example, today one can get multiple credit cards from multiple banks and use them at any ATM in the world without issue.

All multi-party systems need rules to address:

- Operational issues
  - How is the system supposed to work?
  - What are the processes used?
- Technical issues
  - How is the data structured, formatted, communicated, secured, verified, etc?
- Business issues
  - Who can (or is supposed to) do what?
  - What roles exist and what are their duties and responsibilities?

- Legal issues
  - Compliance requirements
  - Risk and loss allocations
  - Warranties and liability

The purpose of these rules is to:

- Make the system **"operationally functional"**, so that it "works", and so that everyone knows what to do and how to design it
- Make the system "**trustworthy**". This, as is explored earlier in this report, goes beyond making the system merely functional. It means to address and minimize the risks, so that participants have confidence in the results and are willing to rely on them
- Address the **legal issues**. This includes:
  - Defining participant legal rights, duties, and obligations
  - Clearly defining and fairly allocating liability risks
  - Filling in gaps not covered by existing law
  - Resolving ambiguous law (e.g. who is liable if "x" happen)
  - Altering inconsistent law (where allowed)

There are three basic categories defining how these rules relate to law:

1 Public law: general law
   a. Existing statutes, regulation, and case law
   b. Not written to address specific system transaction issues
   c. Contract law, tort law, privacy/security law, commercial law, personal injury law, family law, tax law, competition law, etc.

2 Public law: law specific to transaction types - written to address the category of system transactions and applies to all systems of that type. For example, EU eIDAS Regulation, Virginia Electronic Identity Management Act; Reg. Z (for credit cards); Electronic Funds Transfer Act, etc.

3 Private law: governance rules for a specific system (often called trust frameworks)
   a. Written to govern a specific identity system
   b. Visa rules, ACH rules, SAFE-BioPharma rules, etc.

There are various possibilities when considering who would write these rules and the possible governance mechanisms:

- Independent entities formed to govern the system, e.g., Visa, Inc, NACHA
- Founder/controlling participating entities, e.g., UK Cabinet Office for UK.Gov Verify
- Consortium of participating entities, e.g. group of banks
- Informal committee, e.g., InCommon Steering Committee, either elected or appointed by participants
- Vote of all participants
- Ad hoc, e.g., each participant handles independently

In the case of distributed processing, there is no central server that can do everything. Cross-jurisdictional reach is required, transcending state and country boundaries. So, we need a self-regulated system. This is where governance comes in.

Considering the multi-party credit card system, credit card holders have a contract with just one entity. They do not have a contract with other merchants - only with their own bank. Any given merchant has no contract with the bank that issued the card, or anyone else in the system – but somehow it all works.

How do we create this for multi-party systems based on DLT?

Private law - governance rules - can be made enforceable through binding contracts. Saying this, there are also other possibilities for select rules, like performance, custom and usage, software code, or peer pressure.

In cases where user account events are of potential interest to other entities (e.g. to assist in detecting fraud), these shared signals enable intelligence sharing between these entities. Sharing account event notifications could be necessary when, for example, an account credential change is required (e.g., new password), or an account has been purged or disabled.

The Current State of Development of Technical Specifications

The OpenID Risk and Incident Sharing and Coordination (RISC) Working Group is developing technical specifications for shared signals. The initial focus is on internet accounts that use email addresses or phone numbers as the primary identifier for the account.

The purpose of this work is (i) to share information about important security events in order to thwart attackers from leveraging compromised accounts from one Service Provider to gain access to accounts on other Service Providers (mobile or web app developers and owners). And (ii) to enable users and providers to coordinate in order to securely restore accounts following a compromise.

Approaches to Shared Signals System Governance

Bilateral Contracts Model

Here, every participant enters into a contract with every other participant with whom they will transact. This system is the easiest, quickest and most economical to implement. It works relatively well in small multi-party systems.

However, this model requires a contract between each transaction pair, and the number of contracts grows exponentially as the system scales.

Each participant needs a lot of contracts. Rules are embodied in each individual contract, and contracts may vary, so participants cannot always assume that each transaction will be governed by the same rules.

As a result, changes to rules may be impossible to implement universally. There is no trust in the overall system, only in individual contracts.

Trust Framework Model

Every participant agrees once to a common set of rules (e.g., a so-called “trust framework”) that is binding on all participants. Here, rules are embodied in a single trust framework. The same rules apply to everyone so can form a basis of overall system trust. This means that each participant knows how each other participant is obliged to act. When necessary, rules can be changed for all participants uniformly.

> **However, this model involves much more work and greater cost to organize and set up.**

In this new paradigm, businesses have to engage new entities and communities in new ways.

> **There is unallocated risk in the gap between existing ways of operating and the behaviors and activities we are moving towards.**

This begs the following questions:

- *What are the features of blockchain that can help with de-risking the unknowns?*
- *What are the features that can enable consensus mechanisms?*

To this, the ability to share knowledge and monitor information flows is a key feature of blockchain. This increases the trust in and management of the commons. As explored earlier, there are regulations to be developed around shared signals.

> **But markets happen when there are shared metrics. So, regulations and contracts need to be developed around shared metrics too. There is a need to explore the purposes of different metrics and what kind of performance parameters will exist.**

Ordinarily we think about the co-management of assets; co-managing the commons of assets. But, here, discussion was about the co-management of risks; the co-management of the absence of assets, and abstracting these risks in formalized, quantifiable terms.

The Smart Legal Contract Identity Standard and Trust Framework

Accord is a smart legal startup setting standards for smart legal contracts by interfacing with lawyers, industry and technology.

Immutable contracts are still negotiated on paper or PDF. A software system is then typically used to pull important terms out of a contract, making it searchable, digestible, viewable by different parties, and storable. A Contract Lifecycle Management software stack can connect to autonomous blockchain systems, but in many ways this interaction is with a static layer, and involves the following processes:

> *contract request* → *reviewing & redlining* → *approval* → *execution* → *storage* → *records management* → *search & retrieval* → *audit & reporting* → *renewal & disposition*

The following definitions have been offered of Smart Legal Contracts vs Smart Contracts:

“A smart contract is an automatable and enforceable agreement. Automatable by computer, although some parts may require human input and control. Enforceable either by legal enforcement of rights and obligations or via tamper-proof execution of computer code.” -- Clack, Bakshi, Braine, 2016

“Smart contracts are code that is stored and executed on a blockchain. Add a user interface and smart contracts serve as the backends for decentralized applications, or dapps.” -- Mike Goldin, ConsenSys

> **Smart legal contracts are enhanced by real-time data, and software that can be updated. This allows a degree of dynamism, and a wide variety of analytics.**

However, there is a lack of techno-legal standards.

> **Translating contract text (natural language) into computer code is a longstanding challenge in law and computer science, whether domain-specific or general languages that formalize the logic of legal contracts.**

When considering identity transactions in this context, we look at storing, verifying, and transferring identity in the digital world.

The Benefits of Decentralized Identity Systems

Decentralized identity systems empower users with (greater) control over the use of their identity.

These systems are not restricted to relying on one approach, technology, or identity provider that may be a single point-of-failure or suboptimal. They provide the opportunity to employ a greater diversity of approaches and technology. They also offer enhanced security.

Decentralized Identifiers (DIDs)

DIDs, and associated metadata, are globally unique identifiers for decentralized systems. They are persistent - being assigned only once to an entity. They are globally resolvable (interoperable) and offer cryptographic verification of the identifier owner.

OIX could allow real pseudonym services. Currently, these contracts require interpersonal trust.

> **The next step is to allow people to share more relevant information to the domain, which they may feel more comfortable doing because they are able to hide other sensitive aspects of their identity.**

For example, a company might be required to share that their inventory is low, and that they cannot fulfill selling obligations. With DIDs, they can do this without having to reveal proprietary information if they do not want to. Here, pre-contracting is useful. Discovery of information becomes easier because companies and individuals are not obliged to reveal their identities before agreeing to anything.

DIDs are well suited for use in smart legal contracts where there are numerous decentralized entities, and, depending on the context, these entities potentially need the ability to validate a contract identifier.

Different contracts (or clauses) can be authorized to perform specific software services depending on the context, and the performance of contract obligations can be verified by various parties.

When considering smart legal contracts offering a series of verifiable claims, it is noted that contracts establish relationships between, and qualities about, parties and things. Contract clauses often contain a wide variety of legally binding assertions about the characteristics of parties. Contract rights and obligations are a type of quality or achievement.

For example, when a port authority issues a credential to a seller that certain goods have been delivered, a data sensor verifies the credential, which entitles the seller to payment. The specific identifier or whether or not a clause was executed - the status of that contract performance - is updated on the network at a global level.

DIDs and associated data may be read from a distributed ledger. For SLC claims, the distributed ledger may be used to register the issuance of a verifiable claim, as well as verify or revoke the claim.

> **The questions then become: how will these data-driven contracts affect the role of the lawyer? When exploring the relationship between the legal framework and tech architecture, what are the functions and flows between the business people, the attorneys and the tech people?**

This is still an open question, but one can surmise the role of attorneys is not going away in this future. One way this approach can play out is a more engaged and ongoing engagement throughout the lifecycle of legal transactions.

Pillars of Trust - Governance, Identity, Security and Privacy in DLT

Trust frameworks for applications deployed on distributed ledger technology will only be as successful as the integrity of their underlying foundations.

> **The primary elements of trust being: a governance structure with applicable and transparent rules and processes, unique and immutable proof of identification of participants, the highest level of security possible; and, uncompromising privacy for purpose of data classification.**

When developing trust frameworks, the context must be also considered, such as:

- Environment: permissioned vs. permission less, and public vs. private
- Purpose: accounting, provenance, verified claims
- Mechanism: on-chain, or off-chain
- Lifecycle: establish, operate, eliminate

There are some general and widely spread use cases where trust frameworks will be critical to ensuring that parties on all sides of transactions or agreements are fairly represented. These use cases invite further questions that must be considered and deserve some thought. They include: product promises, product liability, monetary vs. non-monetary intent; and, determining conflicts with existing laws and precedents.

Product Promises

With respect to product promises, which are invaluable to an organization’s or company’s brand value, the question that should be considered first is ‘what kind of feature claims and service guarantees can be made?’ by said product.

> **Building a product on top of a decentralized ledger often means less control over external factors, and this can impact the experiences one provides to customers or buyers.**

Furthermore, in a situation where you discover strong evidence that a party is knowingly harming a decentralized ledger your product relies on, with the specific intent to harm the product, what recourse, if any, do you have?

Product Liability

When considering product liability (and, in turn, provider liability), consider a scenario where a business has only made reasonable promises to users, whereby disclaimers are included for any foreseeable issues that reliance on a decentralized ledger may present.

> **In this situation, will the business be able to succeed in disclaiming liability that originates from issues with the underlying ledger?**

In many cases, a product may be a pass-through to interaction with, or storage of, data on a decentralized ledger. Here, where does liability begin and end for data interactions and for data storage on a decentralized ledger that a business or organization helps to facilitate?

Monetary vs. Non-Monetary Intent

Transactions on many decentralized ledgers are market-imputed transfers of asset value. Does intent matter?

> **If a transaction is created for the sole purpose of storing data or performing a non-monetary activity, is the arbiter of the transaction subject to laws intended for financial services companies?**

It is possible that something relayed or handled as part of a transaction has no asset value, but later the market begins imputing a value. In this case, do legal liabilities and regulatory obligations shift under the business, forcing a modification of core aspects of that business to remain in compliance with TOCs and any newly applicable law?

Conflicts with Existing Laws and Precedents

Many types of transactions and state modifications on a decentralized ledger are effectively immutable.

> **How does the nature of a relatively uncontrollable immutable record impact laws that attempt to force the option of mutability? For example, the Right to Be Forgotten, claw back requirements, etc.**

Many products built on decentralized ledgers remove control from external providers and hosts. If users have “digital castles” and possess the keys, does it affect Third Party Doctrine?

What is required of product providers when government seeks access to user data?

These use cases of distributed ledger technology are widely impactful. The questions that arise from the use of this technology need to be addressed so as to ensure trust, and therefore the viability, of transactions and agreements executed on a distributed ledger.

Conclusion

The Blockchain, Identity, Trust and Governance workshop series is bringing a unique opportunity for IT experts and legal thought leaders to determine the most reliable ways forward for the success of initiatives deployed on distributed ledger technologies. The knowledge attained from these workshops with support from the Open Identity Exchange and the Distributed Ledger Foundation will help to inform public and private enterprises on best practices and globally viable governance frameworks to deliver distributed applications successfully and responsibly.

Appendices

Appendix One: Workshop Key Points

- For DLT to be accepted as trustworthy for each use case, close collaboration between technologists and these gatekeepers is crucial at this early stage so that, together, they can design these systems with the necessary protections and legal considerations baked into the technology itself.

- We are likely to see a hybrid approach to structuring smart contracts involving bifurcating contracts into two parts; self-executing code and human prose. For example, a human-language contract will be signed and identically reflected on the DLT, with some automated aspects on blockchain.

- In record keeping and transaction monitoring, DLT provides a uniform base of information on which all parties to a transaction can rely for evidence of the details of that transaction. With DLT, we can expect a reduction of input errors, and the time it takes each participant to verify whether a party has the claimed rights. The increased accuracy of records across markets will lead to a significant reduction in disputes and needless litigation.

- This will succeed to the extent that market acceptance is gained. Participants must be able to rely on DLT to replace existing formats upon which they are already comfortable relying.

- Again, for this, there needs to be a focus on building ties with existing systems; with mediators and gatekeepers on whose trust existing systems function.

- Two use cases of blockchain that are growing at an explosive rate are cryptocurrency and personal data management – i.e. storage, extraction, and exploitation. Each of these two use cases is growing without any sufficient legal framework. It has been suggested that this is partially intentional - a reflection of the libertarian, anarchic thinking of "ask forgiveness, not permission". The result, if this continues, is a legal train wreck waiting to happen.

- The two big issues where greater exploration is needed are*:* the legal status of a blockchain; and, ensuring the security of personal data.

- A default "partnership" scenario, would mean joint liability for all "partners"; governance issues and fiduciary duties, whereby every "partner" has an equal vote (e.g. not through mining power); and potential tax implications, whereby there may be US taxation on all "partners", worldwide. Default partnership rules, if applied to blockchain entities, would be catastrophic.

- One proposed solution is a Blockchain LLC. This would mean:
  - Electing this subcategory of LLC
  - A limited liability shield
  - The technology can be the operating agreement, whereby some form of consensus algorithm is set
  - Authorizing governance on forks and changes
  - Participants could also act for their own account, and in geographic isolation
  - A Sub-C taxation election could be layered on for international treatment, meaning that non-US citizens do not have to pay US taxes.

- The next step, then, would be to define the Operating Agreement.

- The issue of exploitation of personal data is already significant - it already affects consumers. Identity management as a business goes a step beyond OIX to include legal metadata on personal identity management. Here, the company's fiduciary duty is baked into their charter, most notably the notion that the company *has* to be responsible to the consumer. This would be a signal of trust and would set best practices going forward.

- These hot areas of technology will benefit from having appropriate legal framing available - not just regulatory, but also recognized legal structures. These legal framings need to be developed at the State-level for greater integrity.

- In considering multi-party system governance and the shared signals use case, comparison was made to the multi-party credit card system. How do we create this for multi-party systems based on DLT?

- In the case of distributed processing, there is no central server that can do everything. Cross-jurisdictional reach is required, transcending state and country boundaries. So, we need a self-regulated system. This is where governance comes in.

- There are potential issues in shared signals system rules. One lies in the necessity for ubiquitously accepted account event definitions of triggers and meanings, and accepted data formats and timing, etc. There are also issues around privacy and security, confidentiality of information, liability for bad data, IP rights, etc.

- Considering approaches to shared signals system governance, we look at the Bilateral Contracts Model, and at the Trust Framework Model. In the latter, every participant agrees once to a common set of rules that is binding on all participants. We ask here: *What are the features of blockchain that can help with de-risking the unknowns? And what are the features that can enable consensus mechanisms?*

- DIDs, and associated metadata, are globally unique identifiers for decentralized systems. DIDs and associated data may be read from a distributed ledger. For SLC claims, the distributed ledger may be used to register the issuance of a verifiable claim, as well as verify or revoke the claim.

- The questions then become: how will these data-driven contracts affect the role of the lawyer? When exploring the relationship between the legal framework and tech architecture, what are the functions and flows between the business people, the attorneys and the tech people?

- Trust frameworks for applications deployed on distributed ledger technology will only be as successful as the integrity of their underlying foundations.

- The primary elements of trust being: a governance structure with applicable and transparent rules and processes, unique and immutable proof of identification of participants, the highest level of security possible; and, uncompromising privacy for purpose of data classification.

- With respect to product promises, which are invaluable to an organization’s or company’s brand value, the question that should be considered first is ‘what kind of feature claims and service guarantees can be made?’ by said product.

- When considering product liability (and, in turn, provider liability), we must determine, will the business be able to succeed in disclaiming liability that originates from issues with the underlying ledger?

- If a transaction is created for the sole purpose of storing data or performing a non-monetary activity, is the arbiter of the transaction subject to laws intended for financial services companies?

- How does the nature of a relatively uncontrollable immutable record impact laws that attempt to force the option of mutability? For example, the Right to Be Forgotten, claw back requirements, etc.

- What is required of product providers when government seeks access to user data?

Appendix Two: Workshop Agenda

9:00-9:15AM
Welcome: Don Thibeau (Open Identity Exchange & Distributed Ledger Foundation) & Roland Vogl (Stanford CodeX Center for Legal Informatics, and Stanford Program in Law, Science & Technology)

9:15-10:00AM
Panel Discussion: ***The Current State of Blockchain, Law and Governance***
Moderator: Don Thibeau (Open Identity Exchange & Distributed Ledger Foundation)
Panelists:

- Scott David (University of Washington)
- Oliver Goodenough (Vermont Law School & CodeX)
- Bob Robbins (Pillsbury)

10:00-10:45AM
Presentation & Discussion: ***Multiparty System Governance and the Shared Signals Use-Case***
Moderator: Don Thibeau (Open Identity Exchange & Distributed Ledger Foundation)
Presenter: Tom Smedinghoff (Locke Lord LLC)
Panelist: Tony Lai (CodeX & Legal.io)

10:45-11:00AM
BREAK

11:00AM-12:00PM
Presentation & Discussion: ***Accord Project: The Smart Legal Contract Identity Standard and Trust Framework***
Moderator: Tony Lai (CodeX & Legal.io)
Presenter: Houman Shadab (Accord Project)
Panelists:

- Dazza Greenwood (CIVICS.com)
- Meng Wong (CodeX & Legalese)

12:00-1:15PM
LUNCH & NETWORKING

1:15-2:00PM
Presentation & Discussion: ***Pillars of Trust – Governance, Identity, Security and Privacy in DLT***
Moderator: Giles Watkins (Pridium)
Presenter: Daniel Buchner (Microsoft & Decentralized Identity Foundation)
Panelist: Scott David (University of Washington)

2:00-3:00PM
Presentations & Discussions: ***Real-World Use-Cases***
Moderator: Helen Disney (Unblocked)

Governance Model of the Sovrin Foundation Use-Case
Presenter: Drummond Reed (Evernym)

Medical Credentialing Use-Case
Presenter: Eric Fish (Federation of State Medical Boards)

British Blockchain Association Use-Case
Presenter: Helen Disney (Unblocked)

3:00-3:30PM
BREAK

3:30-4:15PM
Panel Discussion: ***Blockchains Incentive, Alignment, and Investing***
Moderator: David Fields (PTB Ventures)
Panelists:

- Eric Fish (Federation of State Medical Boards)
- Professor Jan Liphardt (Stanford)

4:15-5:00PM
Panel Discussion: ***Wrap-up & Path Forward***
Moderator: Don Thibeau (Open Identity Exchange & Distributed Ledger Foundation)
Panelists:

- Scott David (University of Washington)
- Oliver Goodenough (Vermont Law School & CodeX)
- Professor Jan Liphardt (Stanford)
- Bob Robbins (Pillsbury)

Appendix Three: Workshop Speakers & Panelists

Don Thibeau -- Open Identity Exchange & Distributed Ledger Foundation
Don is President and Chairman of the Open Identity Exchange (OIX) and OIX UK/Europe, a non-profit, technology agnostic organization of global leaders from the private and public sectors. OIX is a test bed for business, legal and governance best practices and policies and operates the OIXnet registry. Don is also the Executive Director of the OpenID Foundation, a standards development organization that includes leaders from across industry sectors and governments that collaborate on the development, adoption and deployment of open identity standards. And Don is Acting Chairman of the Distributed Ledger Foundation which is dedicated to establishing the highest standards of trust and governance for distributed ledger technology (DLT). The DLF and its members work together to jointly fund and participate in research and education programs and project initiatives.

Daniel Buchner -- Microsoft & Decentralized Identity Foundation
Daniel leads technical product development for Microsoft's decentralized identity efforts. Previously, he worked at Mozilla, driving Web standards and building open source, developer-focused services, tools, and APIs. Daniel is the Executive Director of the Decentralized Identity Foundation (representing Microsoft) and is working with other members of DIF to realize a decentralize identity ecosystem that enables a new class of apps and services.

Scott David -- University of Washington
Scott is the Director of Policy at the Center for Information Assurance and Cybersecurity at University of Washington and was formerly the Executive Director of the Law, Technology, and Arts Group at UW School of Law. Scott is an active member of the World Economic Forum's Global Agenda Council on Data Driven Development, the MIT/KIT Advisory Board, and the Open Identity Exchange Advisory Board.

Helen Disney -- Unblocked
Helen is the CEO and Founder of Unblocked, a hub for Blockchain events, education, and information. Helen was listed in Innovate Finance's 2016 Women in Fintech Powerlist and referred to by Barclays as a "blockchain guru". She sits on the Advisory Board of the British Blockchain Association and recently gave evidence to the UK's All Party Parliamentary Group on Blockchain. Previously, Helen worked on outreach at the Bitcoin Foundation, driving a programme of strategic events to communicate the innovative potential of Bitcoin and blockchain technology to innovators, entrepreneurs, policymakers, and thought leaders.

Eric Fish -- Federation of State Medical Boards
Eric M. Fish serves as Senior Vice President of Legal Services at the Federation of State Medical Boards. He also assists in the FSMB's federal and state advocacy efforts, analyzing legislation, and consulting on the development of model policies for state medical boards. Prior to joining the FSMB, Ms. Fish served Legal Counsel and Senior Legislative Counsel at the Uniform Law Commission, where aided in the drafting of legislation that reduced the inefficiencies burdening interstate transactions and improve the mobility of people and business across state lines. Mr. Fish holds a B.A. with Honors in Political Science with from the University of Chicago, and a J.D. from Loyola University of Chicago School of Law where he also served as Editor in Chief of the Loyola University of Chicago International Law Review.

David Fields -- PTB Ventures
David is the Founder and Managing Partner of PTB Ventures, a venture capital firm investing in early-stage companies in the digital identity ecosystem. David is a former private equity investment professional and brings over a decade of private investment and advisory experience both to his investors and his portfolio companies at PTB. He began his career as a credit analyst at Citigroup Global Markets and later served on the investment team at Cooper Investment Partners. David graduated from the University of Chicago with a B.A. in Economics and holds the Chartered Financial Analyst (CFA) designation.

Oliver Goodenough -- Vermont Law School & CodeX
Oliver Goodenough's research, writing and teaching at the intersection of law, economics, finance, media, technology, neuroscience and behavioral biology make him an authority in legal innovation. He is currently a Professor of Law and the Director of the Center for Legal Innovation at Vermont Law School and a visitor at CodeX. He is also a Faculty Associate at Harvard's Berkman Center for Internet & Society, a Research Fellow of the Gruter Institute for Law and Behavioral Research, an Adjunct Professor at Dartmouth's Thayer School of Engineering, and a participant in the University of Pavia's initiative on legal innovation.

Tony Lai -- CodeX & Legal.io
Tony Lai is an Entrepreneurial Fellow at the Stanford Center for Legal Informatics (CodeX), where he co-chairs the Blockchain Group, a neutral, collective resource and forum to advance informed perspectives on how blockchain and distributed ledger technologies intersect with existing legal frameworks. As CEO and cofounder of Legal.io, Tony leads a team designing digital identity, referral and review protocols to scale legal access worldwide; working with law firms, regulators and legal service organizations to develop data standards and build client-facing and backend technology for scalable legal service delivery. Prior to Stanford, Tony practiced as a lawyer advising on technology, communications and media industry matters in Europe, Asia and Africa.

Professor Jan Liphardt -- Stanford
Jan is an associate professor of Bioengineering at Stanford University, and the faculty lead for the Stanford Distributed Trust Initiative. Jan is a Searle Scholar, a Sloan Research Fellow, a Hellman Fellow, and the recipient of the 2007 Mohr Davidow Ventures Innovator's Award. Basic research in his lab is funded by federal agencies such as the NCI, NIGMS, NSF, and the DOE. Jan teaches the "Engineering Living Matter" (BioE80) course with Drew Endy, the module on AI/Machine Learning in BioE301C, and a crypto/blockchain class (BioE60 – Beyond Bitcoin: Applications of Distributed Trust). Jan's full publication list is at Google Scholar and his personal blog is here: http://janliphardt.com/.

Drummond Reed -- Evernym
Drummond has spent over two decades in Internet identity, security, privacy, and trust frameworks. He joined Evernym as Chief Trust Officer after Evernym's acquisition of Respect Network, where he was CEO, co-founder, and co-author of the Respect Trust Framework, which was honored with the Privacy Award at the 2011 European Identity Conference. Drummond is a Trustee and Secretary of the Sovrin Foundation, where he serves as chair of the Sovrin Trust Framework Working Group. He has served as co-chair of the OASIS XDI Technical Committee since 2004, the semantic data interchange protocol that implements Privacy by Design. Prior to starting Respect Network, Drummond was Executive Director of two industry foundations: the Information Card Foundation and the Open Identity Exchange. He has also served as a founding board member of the OpenID Foundation, ISTPA, XDI.org, and Identity Commons. In 2002 he was a recipient of the Digital Identity Pioneer Award from Digital ID World, and in 2013 he was honored as an OASIS Distinguished Contributor.

Robert Robbins -- Pillsbury
Robert, Pillsbury's global corporate practice section leader, is recognized as a leader in structuring and closing complex mergers, acquisitions and restructurings, and in advising corporate boards.

Houman Shadab -- Accord Project Consortium
Houman Shadab is co-director of the Accord Project consortium for open source smart legal contract standards. Houman is also a cofounder of Clause and a prolific and influential expert in law, business, and technology with over a decade of background researching and teaching in academia and public policy at New York Law School, Cornell Tech, and other institutions. He has testified before the federal government several times and is widely published and cited.

Tom Smedinghoff -- Locke Lord LLC
Thomas Smedinghoff focuses his practice on the new legal issues relating to the developing field of information law and electronic business activities. Named as one of the National Law Journal's "Top 50 Intellectual Property Trailblazers & Pioneers" in 2014, Tom is internationally recognized for his leadership in addressing emerging legal issues regarding electronic transactions, identity management, privacy, information security, and online authentication issues from both a transactional and public policy perspective. He has been retained to structure and implement first-of-their-kind e-commerce initiatives, electronic transactions, and identity management and information security legal infrastructures for the federal government, and national and international businesses including banks, insurance companies, investment companies, and certification authorities. He has also been actively involved in developing legislation and public policy in the area of electronic business at the state, national, and international levels.

Roland Vogl -- Stanford CodeX Center for Legal Informatics, and Stanford Program in Law, Science & Technology
Dr. Roland Vogl is a scholar, lawyer and entrepreneur who, after more than fifteen years of academic and professional experience, has developed a strong expertise in legal informatics, intellectual property law and innovation. Currently, he is Executive Director of the Stanford Program in Law, Science and Technology (LST) and a Lecturer in Law at Stanford Law School. He focuses his efforts on legal informatics work carried out in the Center for Legal Informatics (CodeX), which he co-founded and leads as Executive Director. Also, he researches international technology law through the Transatlantic Technology Law Forum (TTLF), a think-tank dedicated to transatlantic tech law and policy issues. Dr. Vogl is also a Visiting Professor at the University of Vienna, Austria where he teaches about United States intellectual property law; and a Senior Fellow (by courtesy) at the Berkeley Informatics Lab. Dr. Vogl is actively involved in the rapidly growing legal tech industry. He serves on the board of directors of McCain, Inc. – a company of the Swarco Group; on the advisory boards of IPNexus, Inc., LegalForce, Inc., LexCheck, Inc. and LegalSpace U.S., Inc. In addition, Dr. Vogl serves as a member of the Editorial Advisory Board of Law Technology News, a publication of ALM (American Lawyer Media) and of the Legaltech West Coast Advisory Board.

Giles Watkins -- Pridium
Giles is an experienced board member with a strong Entrepreneurial and Professional Services background. Giles has deep credentials in Mergers & Acquisitions, Finance and Accounting, Technology Strategy, Risk Management, Privacy, Digital Identity, and Cyber Security across multiple sectors and geographies. He is currently working with early stage businesses to commercialise ground breaking technologies and leading the International Association of Privacy Professionals in the UK.

Meng Wong -- CodeX & Legalese
Meng is an entrepreneur, investor, and technologist, specializing in deep-tech internet infrastructure and open-source startups. In 1995, he co-founded pobox.com, an early commercial email service. In 2003 he led the development and global adoption of the email standard SPF (RFC4408). In 2005 he co-founded a venture-funded Big Data startup which was later sold to FICO. In Singapore, he co-founded hackerspace.sg and JFDI.Asia which pioneered startup acceleration in Southeast Asia. His background in innovation is informed by Everett Rogers, Geoffrey Moore, Clayton Christensen, William Janeway, Mariana Mazzucato, and Simon Wardley, and by investing in over 70 startups. He has held fellowships at Harvard's Berkman Klein Center for Internet & Society and at Ca'Foscari University of Venice in computational linguistics. He programs in Perl, Javascript, Prolog, and Haskell.

Appendix Four: Workshop Partners

Swirlds enables developers to create distributed applications with unlimited scope and scale. Leveraging the hashgraph distributed consensus algorithm, developers can build trusted applications that are always available, without the use of central servers. Applications built on the Swirlds platform are fair, fast, and achieve consensus quickly, giving the user 100% certainty in the consensus order. In short, Swirlds provides a platform for building the trust layer of the internet. www.swirlds.com

The Hedera hashgraph platform provides a new form of distributed consensus; a way for people who don't know or trust each other to securely collaborate and transact online without the need for a trusted intermediary. The platform is lightning fast, secure, and fair, and, unlike some blockchain-based platforms, doesn't require compute-heavy proof-of-work. Hedera enables and empowers developers to build an entirely new class of distributed applications never before possible. www.hederahashgraph.com

The Accord Project is the leading organization for the development of standards for smart legal contracts and distributed ledger applications in the legal industry. The consortium operates in collaboration with Hyperledger, the International Association for Commercial and Contract Management, Clio, and a number of leading trade associations, organizations, and law firms. The Project incubates the standard distributed ledger protocol for the legal industry. The purpose of the Project is to enable lawyers, law firms, trade associations, and corporates to help establish open standards for the future of contracting; and to produce open-source code for smart legal contracts and distributed ledger usage by legal and business users. To learn more about the Accord Project, visit www.accordproject.org.

The Decentralized Identity Foundation is focused on building an open source decentralized identity ecosystem for people, organizations, apps, and devices. To learn more visit identity.foundation

The Distributed Ledger Foundation (DLF) is a technology agnostic, non-profit organization composed of business, academic, and legal thought leaders. The foundation is dedicated to establishing the highest standards of trust and governance for distributed ledger technology (DLT). The DLF and its members work together to jointly fund and participate in research and education programs and project initiatives. To learn more www.distributedledgerfoundation.org or ED@distributedledgerfoundation.org

The OpenID Foundation is a non-profit international standardization organization of individuals and companies committed to enabling, promoting and protecting OpenID technologies. Formed in June 2007, the foundation serves as a public trust organization representing the open community of developers, vendors, and users. OIDF assists the community by providing needed infrastructure and help in promoting and supporting expanded adoption of OpenID. This entails managing intellectual property and brand marks as well as fostering viral growth and global participation in the proliferation of OpenID. www.openid.net

PTB Ventures is a thesis driven venture capital firm investing in early-stage companies in the digital identity ecosystem. We believe that digital identity, an evolution that will see trillions of devices connected to billions of humans, will deliver inclusion and security to billions of people while creating trillions of dollars in economic value. www.ptbvc.com