大成 DENTONS

The future of smart contracts

June 15, 2018
Presentation*

STAFFORD MATTHEWS
Partner, Silicon Valley
T +1 650 798 0380
M +1 415 815 9850
stafford.matthews@dentons.com
dentons.com

Why smart contracts and blockchain?

What the Internet does

And does not do.

Why smart contracts and blockchain?

- The **Internet** was originally designed as a peer-to-peer means of communicating **information** rather than as an **e-commerce** platform.
- As it has evolved the Internet has **split** between these two functions.
- The Internet **does** operate as an competitive and transparent means for mass **communication** and **distribution** of **content**.

Why smart contracts and blockchain?

- As a “marketplace of ideas,” the distribution of information on the Internet can be relatively **untrusted.**
- Information is **published by anyone** and everyone in theory can judge for themselves.

Why smart contracts and blockchain?

- But as a marketplace for **goods and services:**

  The Internet has not fundamentally altered the **basic mechanism** of how individual and corporate parties **transact** their business.

Why smart contracts and blockchain?

- The form of the transaction may be **digital.**
- For example, parties may use **email** to exchange **digital copies** of contracts and other documentation, or electronically **transmit** funds, or license and **download** books or films in digital form in exchange for credit card charges.

Why smart contracts and blockchain?

Created by Adrien Coquet
from Noun Project

But most commercial transactions are **not peer-to-peer** and still require a **central** or **controlling authority** or other **“trusted” intermediary** to conduct the exchange.

Why smart contracts and blockchain?

- Where parties who **do not know each other** exchange money for goods and services or otherwise promise to transfer funds or other valuable assets, the **need** for **trust and security** is **high**.

Why smart contracts and blockchain?

- The **trusted authority** may be an online retailer or exchange, or a bank or credit card processor, or a title company.
- Some steps in a commercial transaction may be executed much more efficiently in the digital domain, but the steps are still basically the **same** whether conducted **online** or through **brick and mortar**.

So why?

There are structural **challenges** with the **trusted authority** model which proponents use as **rationales for blockchain**:

- As trusted platforms **scale,** there can be a **concentration** of transactions in a smaller number of key companies acting as trusted authorities.
- For example, in 2016 three online retailers accounted for **65 percent** of all cross-border purchases on the Internet.

Why smart contracts and blockchain?

- Another baseline issue relates to the ownership, collection and use of **personal data** for commercial purposes.
- Use of the trusted authority model requires **disclosure** of personal data to the authority and **retention** and secure **control** of that data by the authority.

Why smart contracts and blockchain?

- Other factors include **new regulatory complexities** that can substantially increase the cost and inefficiencies of doing business in its current form.
- These requirements will result in the need to significantly **scale** the function of the trusted authority and add **more constituent parties** to the transaction, while doing so at **less cost.**

Why smart contracts and blockchain?

- A prime example of this increased complexity is **cross-border manufacturing and distributing** of goods.
- New legal and compliance obligations for **supply chain transparency** require companies to trace, document and report the source of products and their components.*

*See for example the California Transparency in Supply Chains Act of 2010, California Civil Code Section 1714.43.

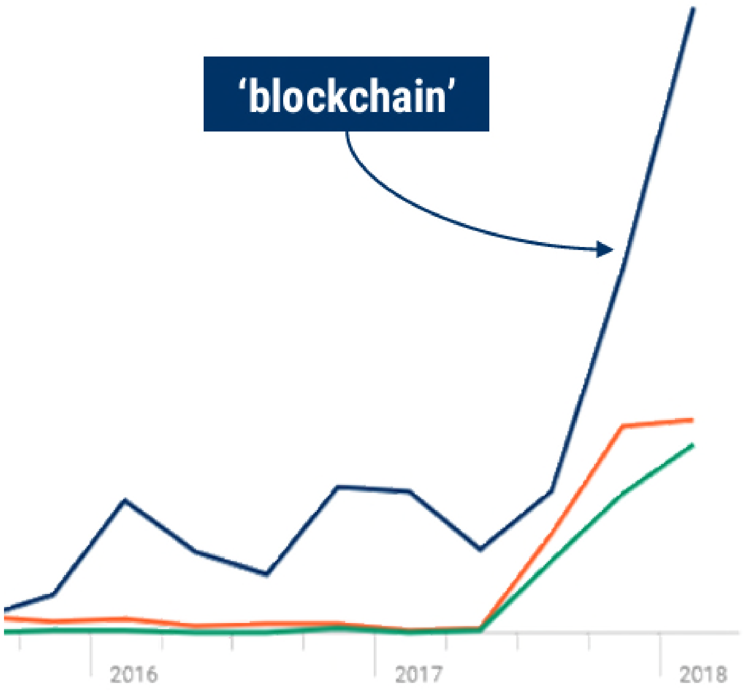
Blockchain as a Solution

The proposed solution to these kinds of limitations is **distributed ledger technology** or **DLT**.

- **Blockchain** is the main iteration of distributed ledger technology.
- Blockchain has been referred to as creating an "**Internet of value**" - as opposed to the Internet of communication.

Blockchain as a Solution - Why Now?

- Through April of this year, “blockchain” was mentioned close to 300 times on Q1 2018 US corporate earnings calls, double all of 2017.



CBINSIGHTS

Blockchain as a Solution - Why Now?

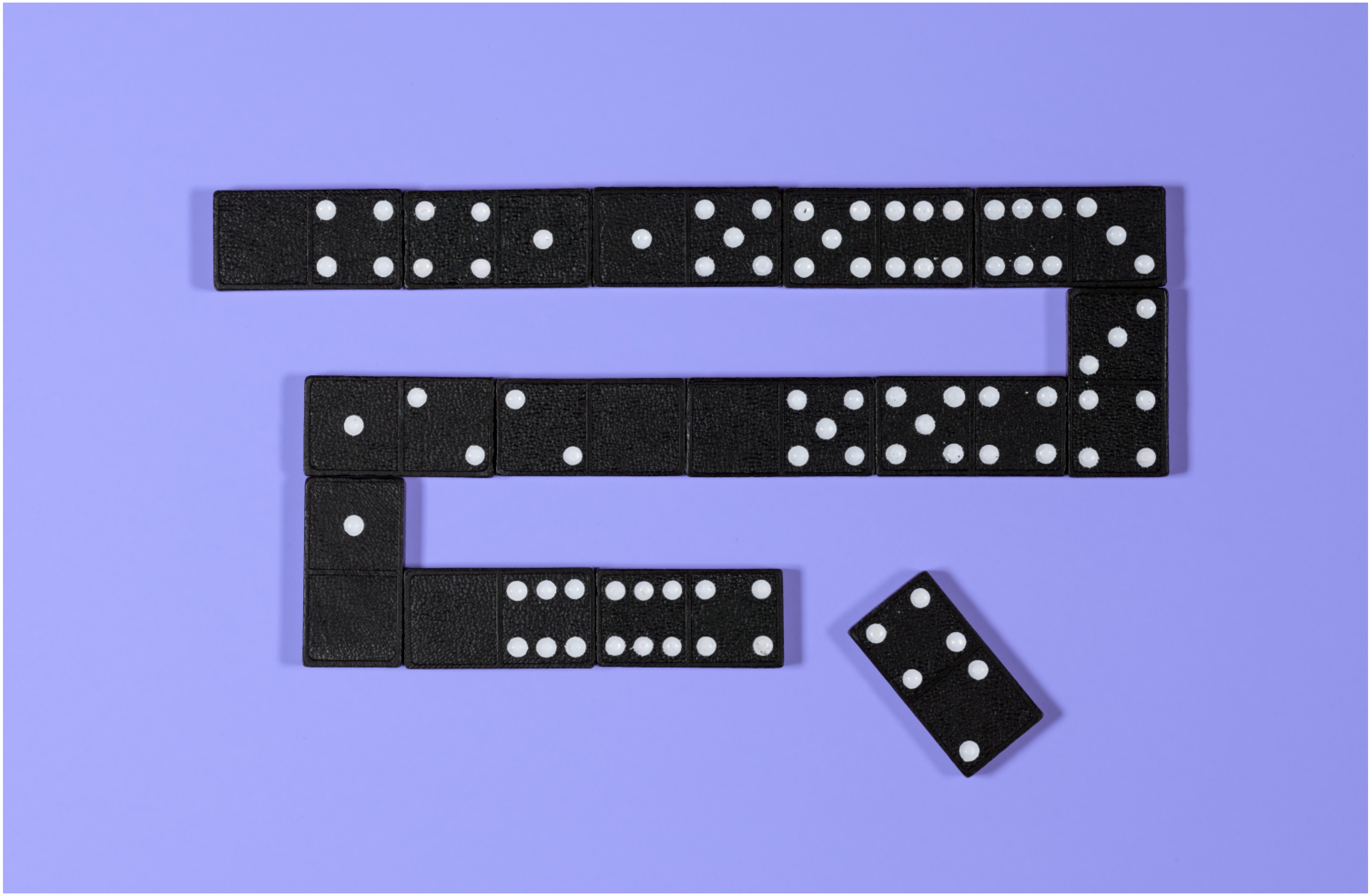
- A survey conducted by Deloitte indicates that **42 percent** of key companies in the consumer products and manufacturing industries plan to invest at least $5 Million in the next year in blockchain technologies.*

*Deloitte LLP, “New tech on the block”, May 2018.

What are blockchain and smart contracts?

Created by Adrien Coquet
from Noun Project

Technology
Innovation
Strategy



What is a blockchain?

Blockchain is

(a) a software **database** that resides on a computer network that

(b) permits all parties within the network to enter into and record **transactions** and other **data** in a linked series of cells

(c) using a **decentralized** and **shared digital ledger**

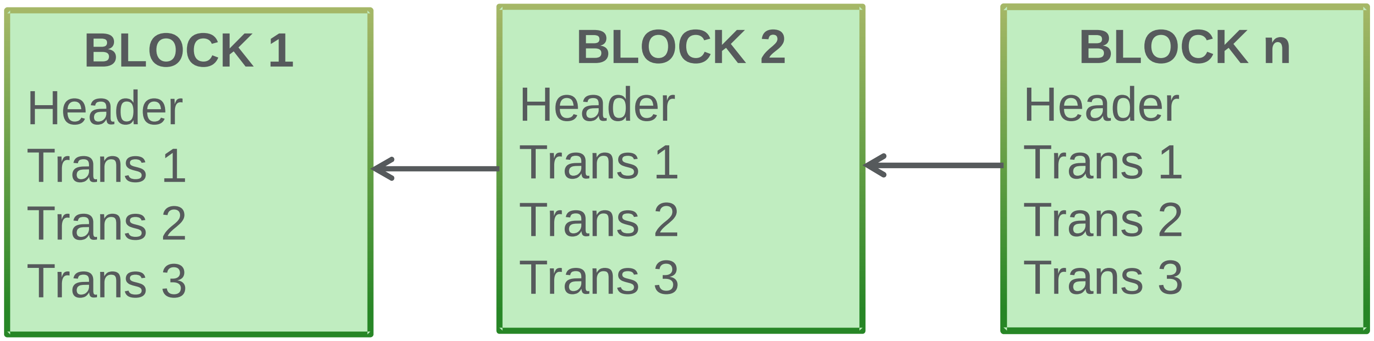
(d) once entered, the data is **immutable** and **cannot be changed**.

What is a blockchain?

- In a pure blockchain there is **no central authority** who decides what goes on the blockchain or holds the only authorized copy of the transaction.
- The core principle of blockchain and smart contracts is that transactions on the network are "**untrusted**". The blockchain – not some authority – contains the record of every single transaction on the network.

What is a blockchain?

- The blockchain holds data on a computer network in a series of cells or "**blocks**" that are **chained** together in chronological time-stamped order.



BLOCK 1
Header
Trans 1
Trans 2
Trans 3

BLOCK 2
Header
Trans 1
Trans 2
Trans 3

BLOCK n
Header
Trans 1
Trans 2
Trans 3

What is a blockchain?

- Each block is **linked to the prior block** using encryption technology known as a cryptographic "**hash**".
- Each block in the chain once linked is **immutable** and can never be modified or deleted. Instead any changes are **written into new cells or blocks** of data attached to the end of the chain.

Adding a new transaction

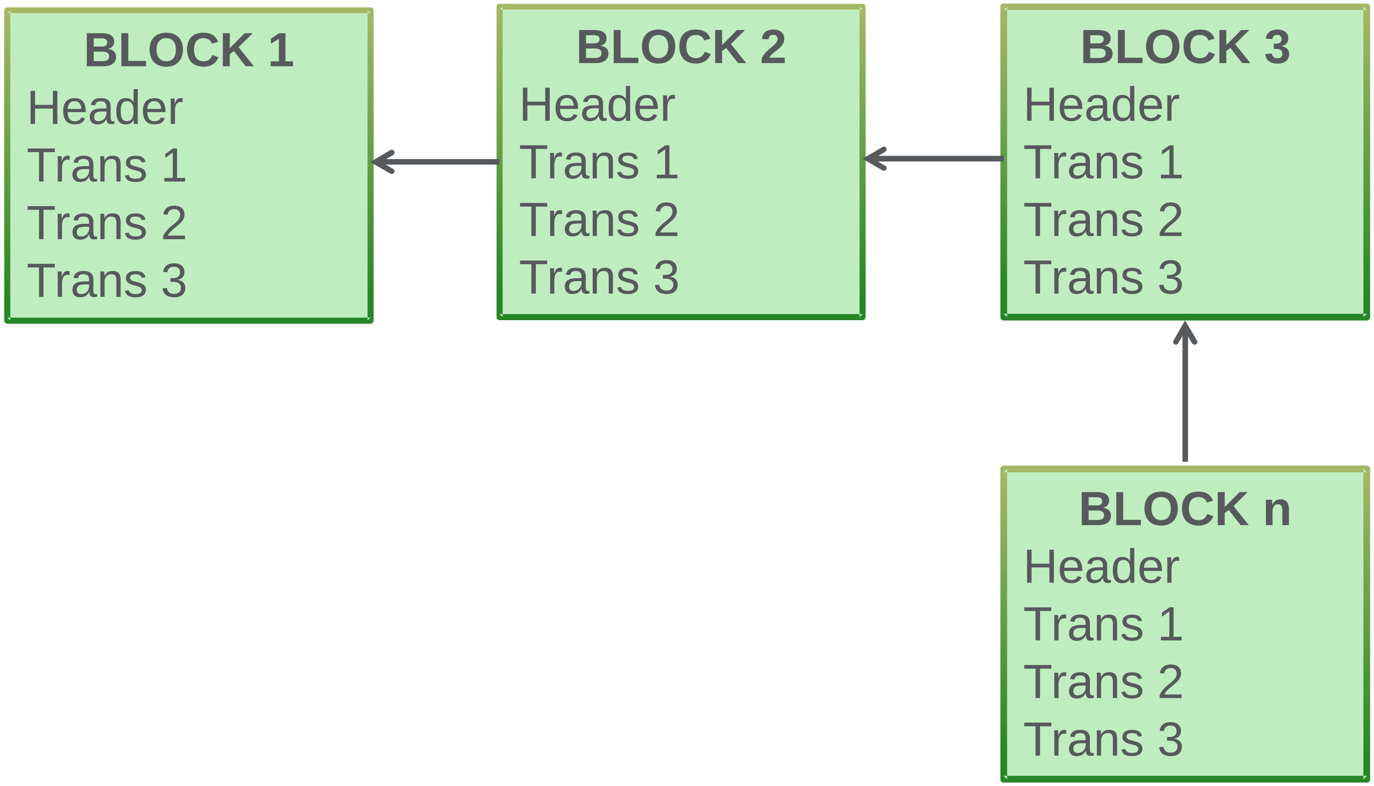
(1) Parties in a **new transaction** first publish the data to the blockchain network.

(2) The computers in the network [known as "nodes"] then compete with each other to **validate** the transaction using pure math.

(3) The validated transaction is then added to a **new block**.

(4) The new block is encrypted and then appended to **end of the chain.**

Adding a new transaction



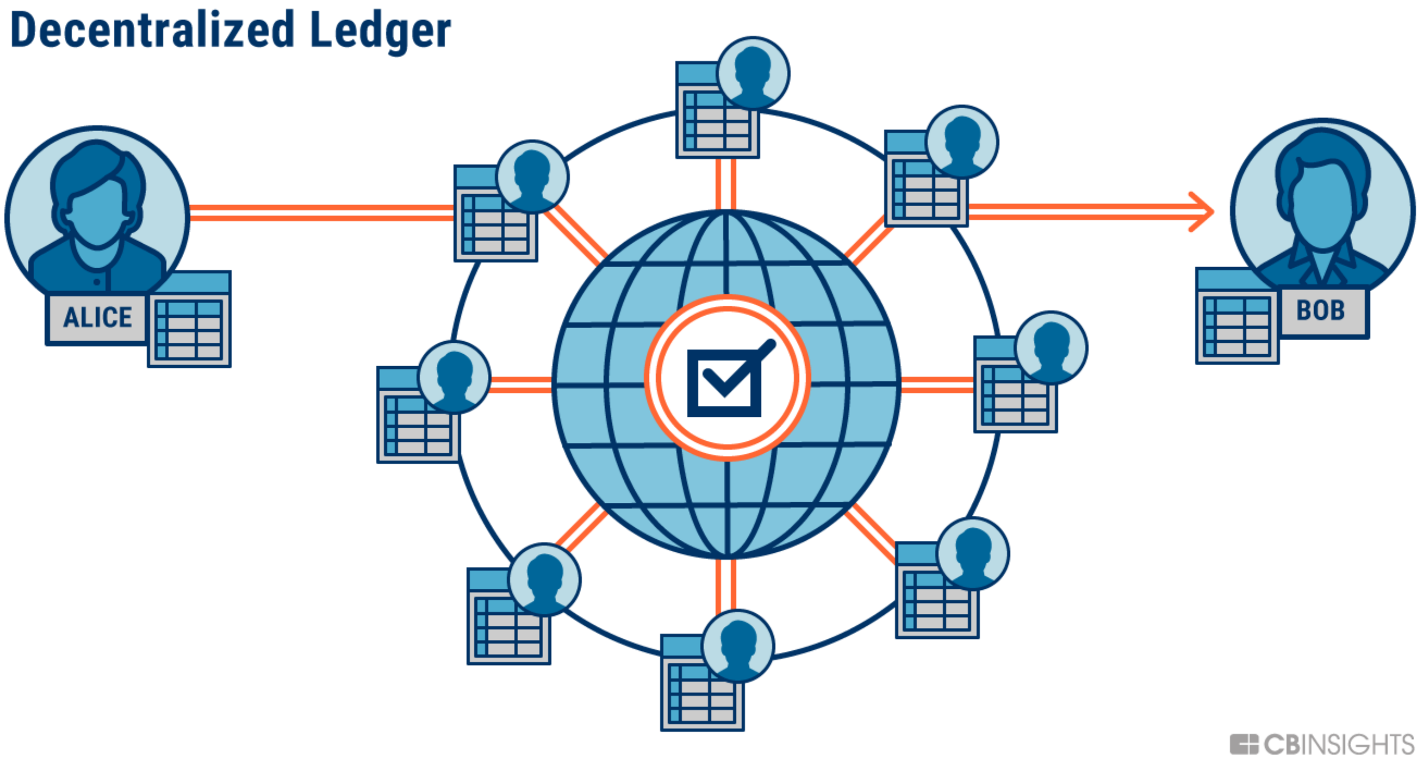
Steps in a blockchain transaction

(5) Exact copies of the then current blockchain ledger containing all of the transactions in the **entire** chain are **updated in real time** and **distributed** to **every computer** in the network on a continuous basis.

Steps in a blockchain transaction

In this manner the entire blockchain database at any point in time is **shared** and **decentralized.** This is the meaning of "**distributed**" or "**decentralized" ledger technology.**

Distributed Ledger Network



Blockchain – What is it good for?

Blockchain has three main categories of uses:

- Creation and execution of **smart contracts**.
- **Peer-to-peer transfer of digital assets** at the human or institutional level, including the creation and exchange of cryptocurrencies such as Bitcoin.
- Storing and validation of **digital records** such as stocks and land title.

Blockchain – What is it good for?

- **Cryptocurrencies** such as Bitcoin are outside the scope of this presentation but have been the main driver of blockchain development at this time.

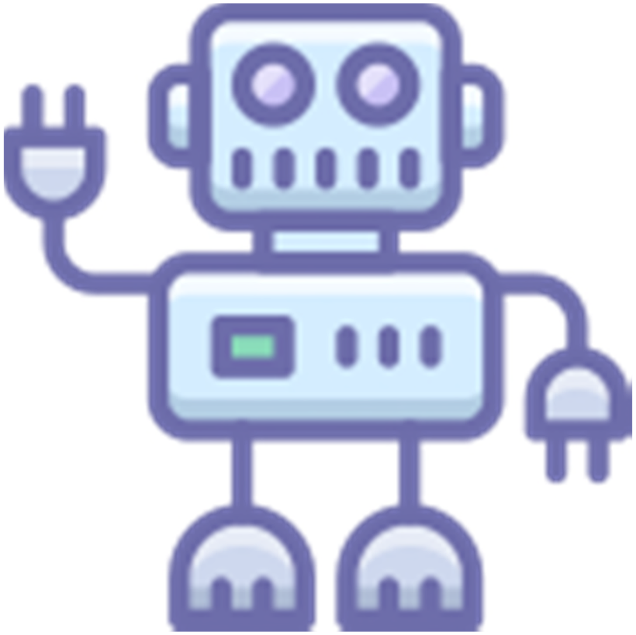
Blockchain – What is it good for?

There are sceptics: Wired Magazine had a May 2018 article entitled "187 Things the Blockchain Is Supposed to Fix“. Wired included the following key Blockchain priorities:

Skynet*
The movie industry's **accounting** practices
Fake news
Authenticity in **cannabis** sales
Paying for things with your **face**

*See The Terminator v. Basically Everybody (1984) et seq.

Blockchain versus Artificial Intelligence



Blockchain versus Artificial Intelligence

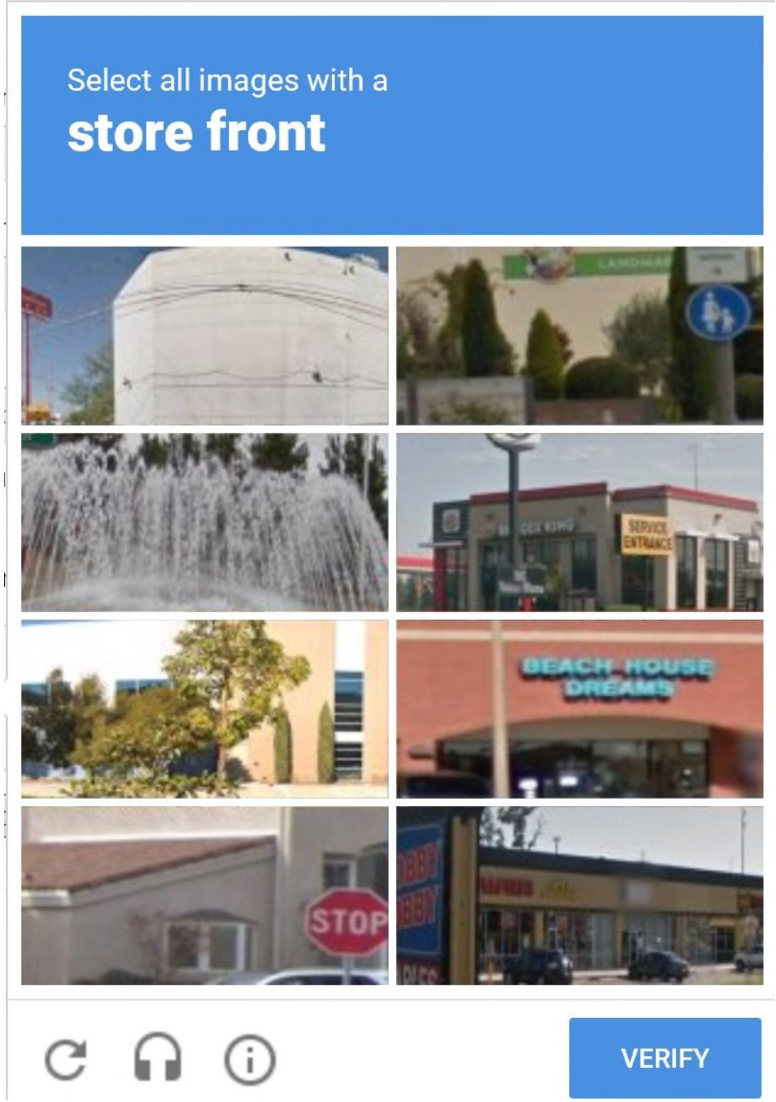
- **Artificial Intelligence** [AI] refers to a set of computer science techniques that enables systems to perform tasks **normally requiring human intelligence**, such as visual perception, speech recognition, language translation, and decision-making.*

*The Economist Intelligence Unit, Artificial Intelligence in the Real World (2016)

Blockchain versus Artificial Intelligence

- **Machine learning** is a **subset of AI** and focuses on the use of **brute computational power** to process and analyze massive data sets in order to develop and improve **algorithms** and models to **predict** future behaviors and outcomes.
- Its focus is **predictive** in nature.

Blockchain versus Artificial Intelligence



Select all images with a
store front

What is a smart contract?

What is a smart contract?

- **Blockchain** technology is not **only** a string of static data records stored in blocks.
- It is possible using certain versions of blockchain software to also store **executable computer programs** within the blockchain to perform functions.
- This executable program can be triggered only by parties holding a **private key code**. This is the basis for building and using smart contracts.

What is a smart contract - 1.0?

- The practical definition of a "**smart contract**" is an agreement using **blockchain** or other distributed ledger technology that is **self-executing**, without the need for further action by the parties.
- Smart contract technology is scalable and autonomous: a form of **robotics for commercial contracts.**

What is a smart contract - 2.0?

Technically more correct to state that a "smart contract" is **computer code**

- embedded in a **blockchain** or other **distributed ledger** that
- incorporates all or part of a written **legal agreement** and
- **automatically** transfers digital assets or vests rights or performs other functions when a set of **pre-defined terms and conditions** are satisfied.

What is a smart contract?

- A physical precursor with some smart contract aspects is the **automated teller machine** [ATM], which issues cash and records transactions as part of a network following a set of instructions and an identification protocol, consisting of

  (1) Insertion of a physical card;

  (2) Input of a secret key code [PIN] known only to the parties.

Why use smart contracts?

As in the case of an ATM machine, the **essential purpose of smart contracts** is to:

- substantially increase **scalability** and **efficiency** of the contracting and performance process,
- while **reducing risk and cost** by the application of **automation.**

Why not use current forms of contracts?

Use of **smart contracting** can:

- Address some **inherent limitations** in structural state of current contracts.
- **Reduce risk** by combining real time data with automated adjustments in the positions of the parties.
- Add **useful components** to the contract toolkit that have not been achievable.

Limits of current contracts

Do Not Scale Well:

- The **traditional “bespoke” legal contract** is currently giving way in various industries towards uniformity and use of **form contracts.**
- **Form contracts** still require the parties to trust each other and require human action to verify and perform their terms.
- Individual contracts also are **“siloed”** and become more difficult to perform and enforce as the number of agreements increases.

Limits of current contracts

Are Static:

- Negotiated and entered into at a particular point in time, even though the contract may be in operation for 5 or 10 years.
- Difficult to **dynamically** interact with and enforce pre-smart contracts based on multiple variables or changed conditions, in particular as the volume of such contracts increases.

Limits of current contracts

Example of the static problem:

- The contract has a term of five (5) years. The limitation of liability clause states that the supplier of critical components has an overall $5 Million cap on all losses in the aggregate during the term of the contract.
- In Year One there is an epidemic product failure and the $5 Million cap is reached. What happens for the next four years if the supplier breaches again?

Limits of current contracts

Example of the static problem:

- Assume instead the supplier fully performs and by Year 5 the purchaser has received 90 percent of the benefits under the contract. Is the $5 Million cap still fair?

Limits of current contracts

Proliferation of Parties:

- As global industries become more complex the average number of counter parties or sub-parties in a transaction has **proliferated**.
- **Smart functions** within a blockchain can include **different levels of assigned permissions** to report and deal with specified transactions and is one solution for **scaling** a larger portfolio of agreements or counter parties.

Limits of current contracts

Verification of Performance:

- Conventional contracts also have no efficient means of **verifying** whether the other party has performed.
- For example, in an IP license agreement the licensor generally must rely on **self reporting by the other party** to compute royalty obligations. There will be a right to audit but that is laborious.

Limits of current contracts

- This may not be an issue for one-off agreements but becomes a **serious logistical burden** when performance is required for a large group or portfolio of obligations.
- Smart license agreements can **automate** the process of obtaining the required information from third parties and **bypass** or at a minimum automatically **corroborate** licensee royalty reports.

Limits of current contracts

Trust Issues:

- Traditional contract models depend upon and trust the **good faith performance** of each party and the **court system** to deliver the benefits of the bargain to each party.
- In addition to the inherent **real world gaps** between parties who do not know or trust each other, this is a particular problem **in cross-border** transactions involving different languages and judicial systems.

Smart Contract Examples

Smart Contract Examples

- **Smart contracts** do not have to be complex and can be used to perform a few **simple functions** repetitively for a large group of transactions or agreements.
- The key to **smart** contracts is their ability to obtain and handle **variable data** and to automatically process and **act** on those variables without the further action of the parties.

Smart Contract Examples

- **Example**: (a) Green transfers **ownership** of securities or other digital assets into the **blockchain**; (b) Blue is required to **pay** $5X for the assets on a certain date, but $8X for the assets if Event A occurs prior to that date.
- The smart contract determines **whether** Event A has **occurred**, and then **self-executes** by (i) paying Green $5X or $8X and (ii) transferring ownership to Blue.

Smart Contract Example: Auto Insurance

Smart automobile insurance policy:

- Sensors in automobile including GPS **track driving behavior** on a continuous basis, including **speeding**, **acceleration**, frequency of **lane changes**, time of day and distance, **use of cellphone** and other corollary data.
- All data would be **continuously added** to the blockchain and recorded permanently along with traffic citations and other external data for each policyholder.

Smart Contract Example: Auto Insurance

- The **smart policy continuously monitors** all of the data in the blockchain.
- The smart policy automatically (i) **increases or decreases** the **monthly premium** for the auto insurance policy based on the data and its built-in algorithms, and (ii) **withdraws** payment from the driver’s bank account.
- The smart contract could compute the premium on a **weekly or even daily** basis.

Smart Contract Example: Auto Insurance

- The smart policy also automatically issues **notices and reports** to the driver, including notice of possible nonrenewal of the policy for poor driving metrics.
- In the case of an **accident**, the smart policy can also obtain data from **vehicle sensors** to do an automated initial **assessment** of damage and even file and process insurance **claims**.

Smart Contract Example: Auto Insurance

- Smart insurance policies can also be **scaled** to **entire companies or fleets**.
- For example, it is possible for ride-sharing companies to use smart **Distributed Autonomous Policies (DAP)** to distribute and operate self-executing insurance policies for their **entire fleet of drivers**, with different terms based on driving record, type of vehicle and other relevant data for each driver.

Smart Contract Example: Auto Insurance

- A scaled smart DAP using GPS could be used to **continuously monitor** and **assess** fleet driver behavior to:
  - Automatically suspend or terminate poor drivers
  - Increase per ride compensation to the best drivers
  - Decrease compensation or redirect drivers in real time where there is excess street congestion.

Smart Contract Example: Supply Contracts

- Assume a **supply contract** for 2000 widgets for $1 Million. The units are required to be delivered by a specified date.
- Buyer agrees to pay **25 percent** of the price on shipment, **25 percent** on delivery and **50 percent** after inspection and acceptance. There is a **penalty** for late delivery not caused by a force majeure. Buyer deemed to accept if units not rejected within 10 days after delivery.

Smart Contract Example: Supply Contracts

Under a smart supply agreement:

- A bank account would be linked to the smart contract. Buyer would deposit **$1 Million** into the account. This would be in lieu of a bank letter of credit or other guarantee.
- Payments would be **automatically made** when the units are shipped or delivered. Confirmation by common carrier including copies of bills of lading would be added to the blockchain.

Smart Contract Example: Supply Contracts

- The smart contract would (i) **continuously track** the units in transit and (ii) **correlate** any delays with **extrinsic data** automatically pulled in from third sources, such as bad weather reports.
- If delivery is late, the smart contract would **execute the penalty** by reducing the payment to the Seller or repaying the Buyer, unless the external data verified a force majeure.

Smart Contract Example: Supply Contracts

- The final **payment** automatically made by the smart contract upon (i) acceptance by Buyer or (ii) no rejection entered into the blockchain within 10 days of delivery.
- If Buyer rejects, then (i) notice of rejection is added to the blockchain, (ii) notice of withheld payment is automatically sent to Manufacturer, and (iii) any dispute resolution mechanisms in the contract are triggered.

Smart Contract Example: Supply Chain

- Objectives: **Coordination of numerous counterparties**; tracking and verification of **source** of components; **supply chain transparency** under applicable law.
- During manufacturing process, bar codes or RFID or IOT devices and other sensors would automatically **identify and track** each **individual component** and upload data to the blockchain for each change in position or state on a real-time basis.

Smart Contract Example: Supply Chain

- The logistics of the product units at each stage of the **supply chain** would be tracked and added to the blockchain by automated means or by counterparty documentation.
- If the **required data not provided** on time, the smart contract will automatically **follow up** with the counterparty.
- The smart contract would automatically prepare and submit all **required filings**.

Other Smart Contract Use Cases

- **Stocks:** Trading and registration of shares of corporate stock. Several states including Delaware have recently enacted statutes permitting use of blockchain as the official stock ledger.
- **Financial Instruments:** Trading of derivatives or other financial instruments.
- **Trade Finance:** Automated issuance of or substitution for letters of credit, guarantees and trade finance instruments.

Other Smart Contract Use Cases

- **Clinical Trials:** Automated obtaining and tracking of required patient consents; standardization of patient inquiries; and secure sharing of personal medical information across institutions.
- **Scientific Research:** Real-time secure sharing of medical or other scientific research between institutions to avoid the “silo” effect; automated nondisclosure terms to protect patent and other IP rights; automatic release of grant funds.

Other Smart Contract Use Cases

- **Self-Sovereign Digital Identity:** Single verified and **encrypted identity** of an individual [KYC] for all institutions and parties in a network.
  - **Degrees of disclosure** of personal information **controlled by the individual** using his or her private key or "authentication tokens".
  - Ability of the **individual** to charge for the use of his or her data.

Building of Smart Contracts

How is a smart contract **constructed** using a blockchain?

Building of Smart Contracts

- There are **competing versions of blockchain software**, similar to competing versions of computer system software such as Microsoft and Apple.
- For example, **Bitcoin** has its own blockchain system for the issuance and transacting of the Bitcoin cryptocurrency as an alternative to fiat currencies such as dollars and Euros.

Ethereum Blockchain System

- The main blockchain software used for smart contracts is **Ethereum**.
- **Ethereum** is a separate open-source, public, blockchain-based distributed computing platform and operating system.
- Ethereum also includes its own cryptocurrency [**ether**] that competes with Bitcoin.

Our Founder

Vitalik Buterin, Russian-Canadian, born January 31, 1994 (age 24 **now**). University of Waterloo [dropped out]. Invented Ethereum at age 19. Net worth > $500 Million.

Ethereum Blockchain System

- The difference is that unlike Bitcoin, the **Ethereum platform** also contains additional critical features:
  - **Smart contract (computer code) functionality** permitting self-executing contract terms and conditions to be embedded in the blockchain.
  - The ability to perform **computations** within the blockchain.

Ethereum Blockchain System

- The ability to obtain **extrinsic or external data** from third parties outside of the blockchain using a function called an "**oracle**".
- The ability to **combine** this external data with the executable computer code within the blockchain to perform smart contract functions.

Other Initiatives

- Ethereum is owned by no one and is an **open system**. The Ethereum Foundation coordinates improvements.
- The **Enterprise Ethereum Alliance** is developing corporate uses for the **Ethereum** blockchain. https://entethalliance.org
- Its **members** include Hewlett-Packard, Microsoft, Credit Suisse, UBS and Cisco.

Other Initiatives

- There are **other initiatives** to bring block-chained based technologies to industrial and financial corporations.
- These initiatives also include the **Hyperledger** project started by the Linux Foundation and supported by IBM and other major firms and banks.

Other Initiatives

- The **Hyperledger** project was established to collaboratively develop open source blockchain systems and tools for various industries and functions.
- These include platforms such as Hyperledger **Fabric** (smart contracts), Hyperledger **Sawtooth** (new proof of consensus) and Hyperledger **Indy** (proof of identity).

Building a Smart Contract: Step 1: Agreement

- Two or more parties must **negotiate** a written legal contract or use a **form contract** from one of the parties or an affiliation group containing their agreement.
- The contract must include specific transactions or other rights and obligations that vest or are executed upon **specified sets** of conditions.

Building a Smart Contract: Step 2: Conditions

The parties **must set**:

- **All of the conditions** to be automated under their agreement
- All **permutations** of each of those conditions
- The **intended result or instruction** in each case.

Building a Smart Contract: Step 2: Conditions

The set conditions can be **internal** to the contract:

- The **manufacture or shipping or delivery** of a product
- A schedule of **due dates** for payments
- **Expiration** of inspection rights or warranties
- A form of **deliverable** or notice by a party.

Building a Smart Contract: Step 2: Conditions

The set conditions can be **external** to the contract:

- Acts or omissions of **third parties**
- Accidents or weather or climate events or other **acts of God**
- Other events of **force majeure**
- Financial or product **market triggers**
- **Changes** in legal or financial status

Building a Smart Contract: Step 3: Coding

- The smart part of a contract requires the writing of a **computer program or code** which incorporates all of the set conditions and intended results, so that the contract will automatically be performed when those conditions are triggered.
- A smart contract therefore always has **two versions:** the human language version and the machine code version.

Building a Smart Contract: Step 3: Coding

Written Contract:

- Human language
- All parts of agreement
- Freely modifiable in writing by the parties.
- Subject to interpretation

Smart Version:

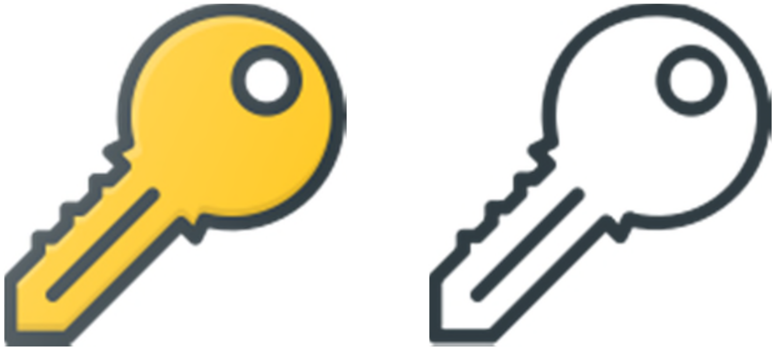
- Machine computer code
- Only transactions to be automated
- Embedded into blockchain or other ledger
- Cannot be changed - only added to.

Building a Smart Contract: Step 4: Blockchain

- The smart contract code is **published** to the blockchain or other distributed ledger network by the parties.
- The smart contract code is **verified** and then "written" into a block in the blockchain or other ledger.

Building a Smart Contract: Step 4: Blockchain

- A **public key** is issued tagging the location of the block where the contract is located.
- A **private key** is issued for each of the parties to the transaction.



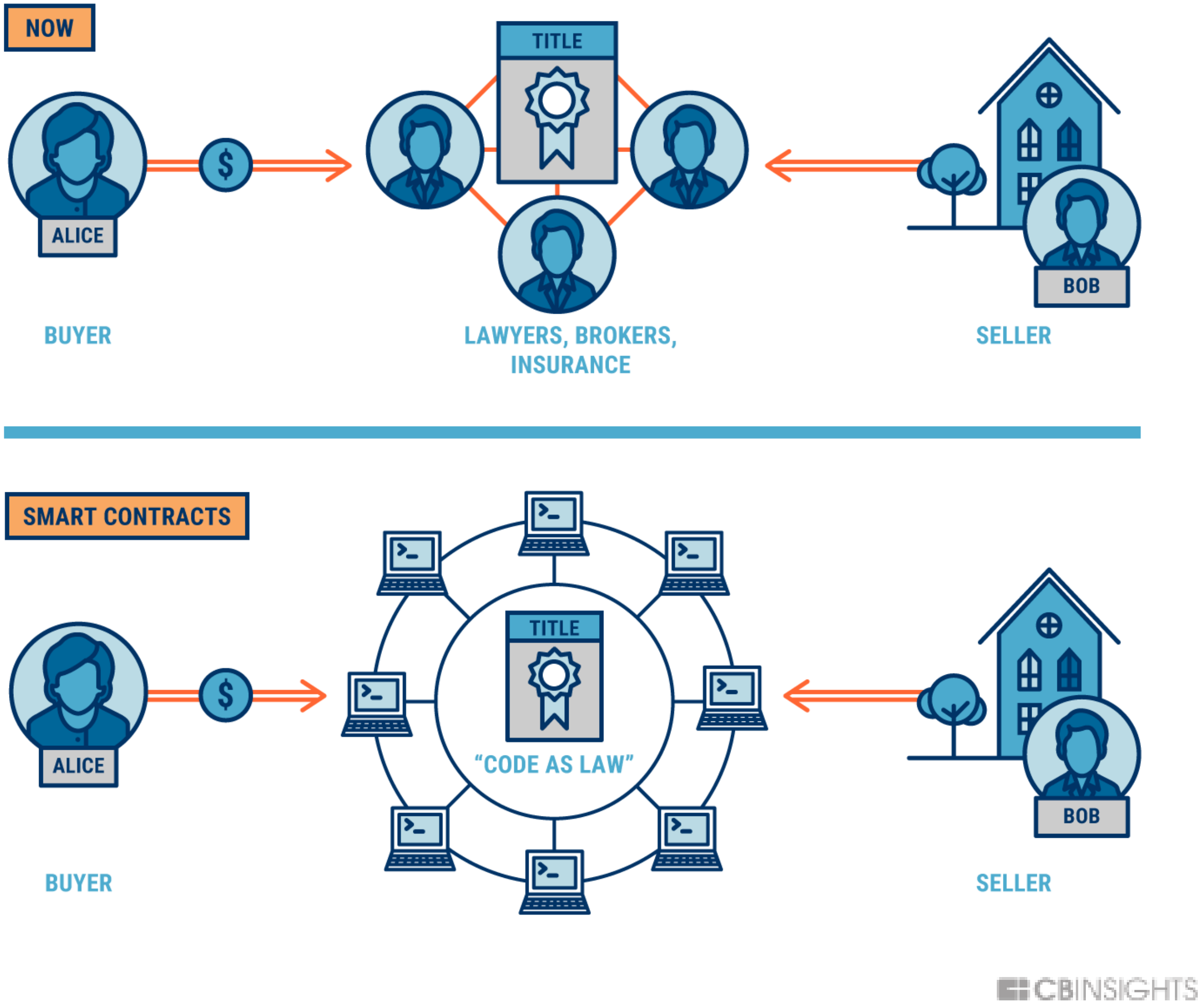
Building a Smart Contract: Step 5: Execute

- **Execution** of the transaction is triggered:
  - by a message sent by a party validated by its **private key** or
  - by the **objective satisfaction** of external or other **events or conditions** coded into the program.
- The transaction [such as transfer of funds or title] is **automatically performed** pursuant to the smart contract code.

Building a Smart Contract: Step 6: Recording

- The **completed transaction** [for example: sale of property; payment of royalties; delivery of shipment] is verified and written into a new block in the chain.
- All of the computers which are part of the relevant network are then distributed **updated copies of the ledger** which show that the transaction is completed.

Building a Smart Contract



Building a Smart Contract

- A smart contract generally will **not be the whole agreement** but only those portions of the contract that are highly **process-based,** can be represented in executable **computer code**, and can be **usefully automated** in a manner that is more efficient and easier to scale than human processing.

Building a Smart Contract

- In its current stage, **better suited to industrial scale** or **repetitive** forms and transactions rather than "one off" agreements.

Where does it go?

- There are basically **three types** of blockchains:

  (1) **Public** or "**permissionless**" blockchains, which are open to the public and are generally fully transparent. Bitcoin and most other cryptocurrencies use this type of blockchain.

Where does it go?

(2) **Group** or **consortium** blockchains, which use a distributed ledger and may have a large number of participants. However under this version, the consensus required to add new transactions to the blockchain is controlled by a **finite set of designated members** or "nodes" rather than all members.   Also known as **"hybrid"** or **"semi-public"** blockchains.

Where does it go?

(3) **Private** blockchains, where the shared database of transactions is limited to a certain **specified group** of participants or parties.

- NB: A **central authority** can be appointed for a private or semi-private blockchain to validate the ledger and keep an "**golden**" copy of the data to maximize core security of the ledger where appropriate.

Where does it go?

- Both consortium and private blockchains are referred to as "**permissioned**" blockchains.

- This is because counterparties and other participants can be granted **different degrees of access and authority** to initiate and interact with the block-chained transaction. Smart contracts used by corporations generally will be in permissioned blockchains.

Legal Issues

There are number of **legal and functional issues** that can arise from the use of smart contracts in their **present stage** of development.

Legal Issues

A. Offer and acceptance

- Parties to a contract must evidence acceptance of the terms and conditions of the agreement.
- There are debates in the relevant circles as to whether existing **electronic signature acts** are sufficient to meet legal standards or whether **additional legislation** is necessary to validate blockchain smart contracts.

Legal Issues

- What rules apply if the statute requires that the contract be "**written**"?
- The Electronic Signatures in Global and National Commerce Act (“**ESIGN Act**”) and the Uniform Electronic Transactions Act (“**UETA**”) and equivalent statutes in several states provide grounds for enforcement of smart contracts once electronically signed.

Legal Issues

- The digital **acceptance** by the parties of a smart contract will need to be by a method evidencing clear **notice** of and an **agreement** to the terms of the contract rather than by mere **implication of assent**.
- Enterprises in particular need to be mindful of the issues of enforceability currently raised by "**browse-wrap"** agreements for online goods and services.

Legal Issues

- A number of courts for example have recently held "browse-wrap" agreements **unenforceable** where the subject party was deemed to not have received sufficient notice of the terms of the contract or to not have consented under the relevant facts and circumstances.*

E.g., Nguyen v. Barnes & Noble, Inc., 763 F.3d 1171 (9th Cir. 2014) ; *Hines v. Overstock.com, Inc.,* 380 F. App'x 22, 24 (2d Cir. 2010); *Cvent, Inc. v. Eventbrite, Inc.,* 739 F. Supp. 2d 927 (E.D. Va. 2010); *Be In, Inc. v. Google Inc.*, 2013 WL 5568706 (N.D. Cal. Oct. 9, 2013).

Legal Issues

B. “Lost in Translation”: Smart Contract Coding

- Written contract terms need to be converted into **computer language** to be embedded as a smart contract in a blockchain. This needs to be done with **complete precision**.
- After a smart contract is added to the blockchain it is immutable and cannot be changed.

Legal Issues

- It is essential that legal counsel and its software coding counterparts establish procedures so there are **no gaps or mistakes** as between the two versions.
- Use of a “**sandbox**” to test and validate smart contract code is necessary before it is embedded in the blockchain.
- Development and use of **preapproved smart contract templates** will limit but cannot eliminate this risk.

Legal Issues

- How does the other side **verify** that the smart contract version prepared by a party is the same as the written term sheet or agreement for the transaction?
- Which party is **liable** in the event of coding errors in the contract?

Legal Issues

C. Security of Smart Contracts

- At this stage of development, there have been some **security breaches** of enterprise smart contracts coded with the principal software language used for Ethereum - at least when smart contracts are posted on a **public blockchain.**

Legal Issues

- Some companies [including Axoni, a capital markets blockchain developer in New York] are proposing a method called "**formal verification**" to test the correctness and security of smart contracts.
- **Formal verification** is an existing rigorous mathematical method used to "harden" software and hardware logic for military, transportation and cryptography computer programs.

Legal Issues

D. Ambiguities of Human Contracts

- There are basic **inherent challenges** in the process of converting from the written contract to the **self-executing** digital one.
- One is the use of **qualifying terms** used continuously to bridge the gap in human language contracts.

Legal Issues

- For example, written contracts contain provisions requiring **good faith** or **reasonable efforts**, **reasonable notice** or other qualifiers such as **materiality**. Other issues include **implied covenants** of good faith and fair dealing.
- Similar to challenges faced in designing and building a fully **autonomous self-driving vehicle.**

Legal Issues

- **New logic and semantics** that objectify and quantify concepts such as materiality and reasonableness will need to be developed before there can be a **fully-autonomous self-executing** agreement.
- Use of **AI** and **machine learning** to develop the logic required.

Legal Issues

E. Irrevocability of Smart Contract Code

- Once the smart contract is embedded into the distributed ledger it is irrevocable and cannot be changed or deleted and will be **self-executing**. This is the equivalent of a **transactional doomsday machine.**
- This can be **corrected** by the parties adopting and embedding a **revised** smart contract to supplement the existing block-chained one **but only if both agree.**

Legal Issues

What happens when there is:

- A **mistake** of law or fact.
- Other **defects** in the underlying written contract or in the smart contract or there is a **dispute as to meaning or performance** and the parties do not agree to correct.
- Unanticipated **future events**, such as bankruptcy of a party.
- **Fraud** in the inducement.

Legal Issues

- Under discussion are the required use of “**kill switches**” in smart contracts that would **prevent self-execution** if:
  - One of the parties files for **bankruptcy**
  - A court of law issues an **injunction** against performance of the contract.
- Without a kill switch or other similar mechanism, how do you **stop** the smart contract from self-executing?

Legal Issues

F. Jurisdictional Issues

- Which is the **controlling** agreement: written or digital?
- Enforceability of smart contracts in **cross-border** transactions when different rules apply in the relevant jurisdictions, including choice of law provisions.
- What is the **location** of the smart contract for jurisdictional purposes?

Legal Issues - The End Times

G. Rise of the [Uniform Contracts] Machines

- The **front end complexity** associated with building out smart contracts will accelerate the drive to adopt **uniform contracts** in industries: to maximize **interoperability** and **scalability** just as with any other **standard technologies** [see: electric plugs; mobile cellular transmissions; DVDs].

Legal Issues

- **Growing convergence** in standardizing commercial contracts such as non-disclosure agreements [NDAs], supply agreements, online terms and conditions.
- **Certain industries are already there**: ISDA [International Swaps and Derivatives Association] standard agreements for certain financial transactions; NVCA [National Venture Capital Association] model legal documents for startups.

Legal Issues

- It is inevitable that **smart contract and distributed ledger technologies** will accelerate this convergence to uniform contract standards.

#

"The desire for safety stands against every great and noble enterprise.”

— Tacitus, 100 AD

STAFFORD MATTHEWS

Partner, Silicon Valley
Dentons US LLP
1530 Page Mill Road, Suite 200
Palo Alto, California 94304 USA
T +1 650 798 0380
M +1 415 815 9850
stafford.matthews@dentons.com

Dentons is an international legal practice providing client services worldwide through its member firms and affiliates. This publication is not designed to provide legal or other advice and you should not take, or refrain from taking, action based on its content. Please see dentons.com for Legal Notices.