Blockchain

INDUSTRY PRIMER
The LDR Advantage

SWOT Teams

FAST & FLEXIBLE SWOT TEAMS

- 3-5 person teams with diverse skill sets in finance, legal, marketing, strategy, insurance, and operations.
- Teams flex based on client need.
- Rapidly deployable, self-sustaining teams capable of conducting an array of operations: deal advisory, strategic initiatives, management consulting, due-diligence, and project management.

FULL-SPECTRUM EXECUTION

- LDR philosophy built on: (i) military doctrine, (ii) agile methodologies and (iii) combat leadership that taught the achievement of objectives through teamwork, precision, and speed.
- Unique methodology and flexible SWOT teams enable execution on a diverse variety of initiatives.
- Incentives are aligned with major shareholders - eliminates the risk.
History
Bitcoin and Blockchain

Understanding blockchain begins with understanding Bitcoin, as blockchain was born out of the vision for Bitcoin. Bitcoin software was launched in January 2009 to create a digital currency that could be transferred directly between two or more parties without the need of a central authority (e.g., the banks). This disaggregated transactional system depended on the existence of a mechanism that could step into the place of a central authority to validate transactions, avoid fraud, and eliminate the risk of double-spend.

Blockchain was designed to facilitate a wide variety of transactions in addition to cryptocurrencies such as escrow transactions, bonded contracts, third-party arbitration, and multiparty signatures. Now that industries are beginning to apply blockchain to non-crypto currency use cases we have entered the era of Blockchain 2.0. Whereas Blockchain 1.0 was for the decentralization of money and payments, Blockchain 2.0 is for the decentralization of markets more generally.

October 31st, 2008
The Bitcoin White Paper was Published

February 9th, 2011
Bitcoin reached parity with the US dollar

October 31st, 2009
“The Bitcoin Market” was established

January 26, 2016
The Linux Foundation charters Hyperledger to promote the creation of open source blockchain projects.

December 2013
The Ethereum Project white paper was published. Beginning of Blockchain 2.0

November 29th, 2017
Bitcoin value surpasses $10,000
What is (a) Blockchain

Blockchain is a technology, not a company, and more specifically is a public ledger of all transactions executed within a network. The ledger is replicated on all nodes (computers) that update in real time in a peer-to-peer network. Data is shared equally and not controlled by a central entity. Most participants can write and read the data on the blockchain.

Blockchains can be defined by who is able to view the ledger and who is involved in the verification of transactions.

- **Public**: No restrictions on reading blockchain data (which still may be encrypted) and submitting transactions for inclusion in the blockchain.

- **Private**: Direct access to blockchain data and submitting transactions is limited to a predefined list of entities.

- **Permissionless**: No restrictions on identities of transaction processors (i.e., users that are eligible to create blocks of transactions).

- **Permissioned**: Transaction processing is performed by a predefined list of subjects with known identities.
Block-Chains

Blockchain makes sophisticated use of hashing and cryptography to create an unalterable chain of transactions that is validated by certain sophisticated participants (computer nodes) and viewable by all in the network.

Individual blocks on the chain are constructs that group every transaction that occurs within a network over a given time period.

Blocks are created and verified by a mechanism that aims to achieve consensus from the majority of participants in the network concerning the legitimacy of the transaction. The type and amount of verification can be different for each blockchain, depending on its protocols.

Source: Making sense of bitcoin, cryptocurrency, and blockchain, PwC
Block-Chains

Hashing and the linking effect are the foundations of blockchain's security. Hashing algorithms produce a unique fingerprint - a digital signature - that cryptographically represents the contents of a block. Each block is linked to the previous block, creating a chaining effect that cannot be decrypted or altered, providing a publicly accessible, permanent and encrypted digital record. This linking effect creates a tamper-proof ledger.

Changing a transaction (input) will change a block’s hash (output), breaking the link between the adjacent and all subsequent blocks.

The most popular consensus mechanism is "proof of work" as utilized by Bitcoin. New blockchain platforms are using other consensus mechanisms (i.e. alternatives to proof of work) and more will be created to reduce computing power, electricity, and cost.
Blockchain technology can fundamentally do 3 things:

1. **Storing digital records**
   Allows unprecedented control of information through secure, auditable, and immutable records of transactions and digital representations of physical assets.

2. **Exchanging digital assets**
   Issuance of new assets and transfers of ownership in real time without banks, stock exchanges, or payment processors.

3. **Executing smart contracts**
   Self-governing contracts simplify and automate lengthy and inefficient business processes. Smart contracts allow for digital implementation and verification of the clauses of a contract.

Source: Deloitte University Press
Smart Contracts
Self Governing and Automated

Smart contracts are built on computer code that links the automatic performance of certain contracts. The coded contract can reflect any kind of data-driven business logic. When an event prescribed in the contract happens, the code (or clause) is executed and verified by the network of computers on the blockchain. This computer code is stored and run on a blockchain. The result is stored as a transaction log representing the transfer of digital assets or value between the parties involved.

![Smart Contracts Diagram]

Source: Smart Blockchain Contracts: Are We Finally Going Paperless?, Kepler Cannon.

The prescribed event or trigger of a smart contract can be a transaction on the blockchain, or inputs from an external source. External inputs are retrieved from off-chain data sources known as "smart oracles" that evidence the event in question.

**Triggers (Smart Oracles)**

- Software
- Hardware
- Inbound
- Outbound
Immediate Commercial Impact
Accountability and Efficiency

Immediate commercial applications are those that improved **accountability** and **efficiency** for moving goods and performing services.

**Accountability**: Poor information and limited visibility plagues the global supply chain. Social, regulatory, and environmental pressures force a transparent and traceable supply chain. Blockchain makes this otherwise cumbersome tracking process easy.

**Efficiency**: A shared and publicly viewable ledger creates efficiencies in administrative tasks, transactions, and coordination along the supply chain, as well as in the delivery of professional services, and the administration of contracts.

*Source: Fast Forward - Rethinking Enterprises, Ecosystems and Economies*
Know the Risks to Win

Dotcom Failure

Risks:

**Scalability:** The computing power required is the primary barrier to scalability. Bitcoin (fueled by blockchain) can only process 7 transactions per second (TPS), while Visa averages 2,000 TPS and Paypal 193 TPS.

**Regulations:** The position of regulators on blockchain is unclear, creating confusion and uncertainty.

**Collaboration:** The value of blockchain depends on the number of participants in the network and the data contributed to the ledger (i.e. smart oracles). This hinges on practical and commercially viable use cases and will require collaboration between competitors, suppliers, customers, manufacturers, and others.

Characteristics of Winners:

Blockchain will be an important tool to act as a single, verifiable source of truth. Blockchain can be immediately most successful in areas that need tamper-proof records, different levels of access and security, and an audit trail for traceability. Blockchain also provides value where disintermediation leads to efficiencies. Lastly, blockchain is best used in transactions that previously required the assurance of a third party to validate the provenance of a good but are burdened by the costs of acquiring these assurances.
Blockchain Use Cases

Case Study 1: Diamonds - Everledger
Blockchain helps establish a trusted provenance in the diamond industry that is plagued with counterfeit gems.

Case Study 2: Brazilian Beef - Beef Tools
Growing global demand for beef led to deforestation of the Amazon Rainforest. Blockchain provides traceability to hold beef suppliers accountable to regulators and consumers.

Case Study 3: Counterfeit Pharma - Chroniced
The counterfeit drug industry is massive -- $200b -- and poses massive risks to consumers and governments. Blockchain provides transparency and traceability to secure the pharmaceutical trade.

Case Study 4: Solar Energy Sales - Brooklyn Microgrid
Blockchain is being tested as an alternative to the traditional power distribution model. A local energy grid allows participants to generate and exchange power in a permissioned peer-to-peer network.

Case Study 5: Identities - Evernym
Paper identities can easily be lost, stolen, or duplicated. Blockchain provides a way to securely issue these documents.
Diamonds

Case Study One: Everledger

Current Scenario:

The diamond market uses paper certificates to ensure the authenticity of the stones. These certificates can easily be lost, duplicated, or destroyed. This creates many opportunities for fraud, theft or counterfeiting of gems. Stakeholders in the diamond industry want traceability to the source and are unable to do so reliably.

Incentive to Adopt

- $50 billion in fraudulent claims annually;
- Unethical treatment of humans (blood diamonds); and
- Counterfeit gems

Blockchain Solution:

- Everledger’s blockchain allows everyone on the digital market to see exactly where the diamonds have been ensuring ethical trade and helping eliminate the blood diamond market.
- Everledger’s blockchain is a unique public/private hybrid with the transparency of a public chain and the permissions of a private one.
- Each diamond has an inscribed serial number. This number is combined with forty other diamond characteristics to create an identification code on the blockchain. This identification code acts as a digital signature to trace the diamond from source to use, replacing paper records to ensure the authenticity of the gem.
- This prevents counterfeit and fraud, and makes it nearly impossible to sell a diamond outside the black market.
- Over a million diamonds have been uploaded to the database.
Brazilian Beef
Case Study Two: Beef Tools

Current Scenario:
Rising demand for beef encouraged deforestation of the Amazon in Brazil. Consumers, governments, NGOs, and others have demanded action to protect such a critical part of the world ecosystem. However, the complexity, burden, and cost associated with monitoring supply chain activities (creating, updating, maintaining databases) meant it was difficult to enforce accountability and change behaviors. Large suppliers and retailers of meat had undertaken enormous and costly efforts to trace their supply chain. Meatpackers struggled to prove they were processing deforestation free-beef.

Incentive to Adopt

- Fine for having cattle in a prohibited area of the Amazon (26 beef producers faced fines of $282 million for raising cattle in this region in 2013);
- Decreased CO2 levels. Amazon deforestation is a driver of global warming; and
- Consumer and regulatory pressure to verify beef is sustainably produced.

Blockchain Solution:

- Blockchain offered an elegant solution. A private consortium developed a blockchain that enabled retailers and grocers to trace cattle to from the source to ensure the farm was deforestation-free.
- Previous efforts to create a shared database failed due to meatpacker’s reluctance to share valuable supplier information. Blockchain’s access permissions solved this and enabled all parties to verifiably trace the movement of cows along the supply chain.
- Blockchain — a shared, trusted, and secure database -- provided an information service for large companies that must prove to consumers and regulators they are selling sustainable beef.
Counterfeit Pharma
Case Study Three: Chronicled

Current Scenario:

Counterfeit drugs plague the pharma industry. It is difficult for organizations to identify which companies are responsible for fake drugs because each maintains its own internal database. This makes it hard to rectify discrepancies and easy for drug to be lost in transit. The FDA’s Drug Supply Chain Security Act calls for the pharma supply chain to create an “electronic, interoperable system to identify and trace certain specific drugs as they are distributed in the United States”—with compliance expected to be completed by 2023.

Incentive to Adopt

- $200 billion worldwide counterfeit drugs annually;
- One million people die each year from counterfeit drugs; and
- Prescription drug abuse.

Blockchain Solution:

- Chronicled was founded in 2014 with a mission of providing cryptographic identities for physical things.
- It is currently working on the MediLedger Project which aims to manage pharmaceutical supply chains. This allows companies to record drug deliveries on the blockchain.
- During each step of the distribution, process computers will verify the provenance and authenticity of the drug shipment. This will make it harder to steal drugs and easier to identify who is accountable if they are stolen.
- Chronicled’s tamper-proof sensors will ensure that the drug packaging is not broken before it reaches its owner, ensuring the pills are not counterfeit.
Solar Energy
Case Study Four: LO3 Energy

Current Scenario:
LO3 Energy, a Brooklyn-based energy startup, is running an alternative to the traditional power distribution model. This community based energy grid, BMG, allows participants to generate, store, buy, and sell energy at a local level. This is done primarily through PV (photovoltaic systems) which operate on a microgrid that runs parallel to the main grid.

Incentive to Adopt

- **Consumer-Centric**: Peer-to-peer purchases of electricity are more cost-effective as the transactions can be made in small amounts and without intermediaries.
- **Environmental Benefits**: The traditional energy grid is supplemented with community-sourced power. This allows for greater accessibility of clean, renewable energy.
- **Disaster Resiliency**: Microgrids can retain functionality even in the event of the main grid shutdown.
- **Tailored Regulations**: Regulatory reform can reward certain transaction behaviors, like purchasing local power.

Blockchain Solution:

- Blockchain technology allows devices at grid edge to securely and directly transact for PV-generated energy sale among microgrid participants.
- Blockchain allows peer-to-peer energy sales to be tracked and recorded.
- Soon, users will be able to set preferences that dictate their local grid energy exchange with their main grid-supplied energy, ultimately choosing their energy sources. This will be carried out through self-executing contracts in the blockchain.
Identities
Case Study Five: Evernym

Current Scenario:

Even governments, in Illinois and Switzerland, are starting to make use of blockchain technology to manage citizens identities. Paper identities can easily be lost, stolen, or duplicated, and online identity theft plagues consumers. This month, the city of Zug, Switzerland, launched a project in collaboration with uPort, a startup whose identity management system relies on the Ethereum blockchain, to provide self-sovereign IDs to its citizens.

Incentive to Adopt

- Reduced fraud and identity theft;
- Reduced administrative costs and delays to process transactions; and
- Improved delivery of government services.

Blockchain Solution:

- Evernym is using blockchain to create digital ID’s for citizens of Illinois to manage and secure their identities.
- An individual’s identity attributes (legal name, birthday, sex, blood type, etc) are encrypted on a distributed ledger, and only the owner of the digital key can access them.
- A digital ID can be easily and securely validated by authorities, without the need for a central repository.
- Similarly, Zug and uPort are working to create and store secure, distributed identities for individuals. uPort is building on the Ethereum blockchain as Zug wants to digitize transactions such as voting, ticket payment, and e-signatures.
LDR is an innovation consulting firm focused on providing advanced problem solving, leadership, and investment acceleration services that help businesses achieve their goals. LDR operates as a conduit between capital providers and invested companies to seize opportunities, develop innovation capabilities, and accelerate operations with the goal of maximizing ROI for all stakeholders. To learn more, visit www.LDRinvest.com.