scottmadden
MANAGEMENT CONSULTANTS

Smart. Focused. Done Right.®

Blockchain: An Introduction for Executives

Making Sense of the Buzzwords

Fall 2017

Table of Contents

scottmadden
MANAGEMENT CONSULTANTS

"You never change things by fighting the existing reality. To change something, build a new model that makes the existing model obsolete."

– R. Buckminster Fuller

Background

The world is growing more decentralized, in large part due to the transformative power of the internet.

- While originally thought to be isolated to use cases such as email and news media, the internet laid the foundation for unprecedented, multi-billion dollar industries and innovations such as ecommerce, social media, the cloud, smartphones, and online gaming
- However, the internet also enabled activities like identity theft, unwarranted surveillance, and the monopolization of personal data
- Blockchains bring security and privacy to the decentralized, digital world potentially addressing many of these undesirable consequences of the internet

Blockchain technology carries a similar revolutionary potential to that of the internet, though be wary of the hype.

- By making certain data immutable and shared across a network, blockchains allow value to be digitized, exchanged, and recorded without the facilitation (and cost) of a trusted third party – something truly unprecedented
- This means that any industries not already disrupted by the internet whose services include data collection, curation, verification, and/or dissemination could now be disrupted, especially those that are currently centralized and monopolized (e.g., banking)
- This also means that services previously susceptible to malpractice once digitized (e.g., voting and music sharing) can now be safely and securely brought into the 21st century
- And finally, this means that the tedious activities associated with data silos and imperfect communication, like filling out a medical history form every time we visit a new doctor, can be things of the past. We can now make (and own) one record that's stored on an immutable, append-only blockchain, and anyone we select can reference our record anywhere at any time
- Despite this awesome potential, we are still very much in the early 90s of the blockchain adoption and development curves. Much work has yet to be done as the technology matures, and business cases are only beginning to be flushed out. The priority now is to learn and pursue low-risk pilots

SOURCE: CoinDesk

Key Findings

Digital trust is expensive. Blockchains can makes it unnecessary.

- With blockchains, the trust we ordinarily rely on to exchange goods and services online is replaced by a single shared system of record that maintains all transactions, past and present, as well as the rules by which those transactions are governed
- These omniscient records consolidate the functions of markets, contracts, and ledgers into secure, automatable platforms with no centralized points of control
- As foundational technologies, their purpose is to reduce transactional friction and provide the infrastructure required to build new, potentially disruptive applications

Three takeaways

- Blockchains are customizable, decentralized digital ledgers maintained by a network of peers using well-established cryptographic techniques
- Blockchains operate through network consensus to record and manage anything of value, including identities, assets, and data
- Blockchains enable unprecedented coordination in competitive environments, which lowers transaction costs while increasing transaction speeds, distributing risk, and creating new opportunities to develop value-added services

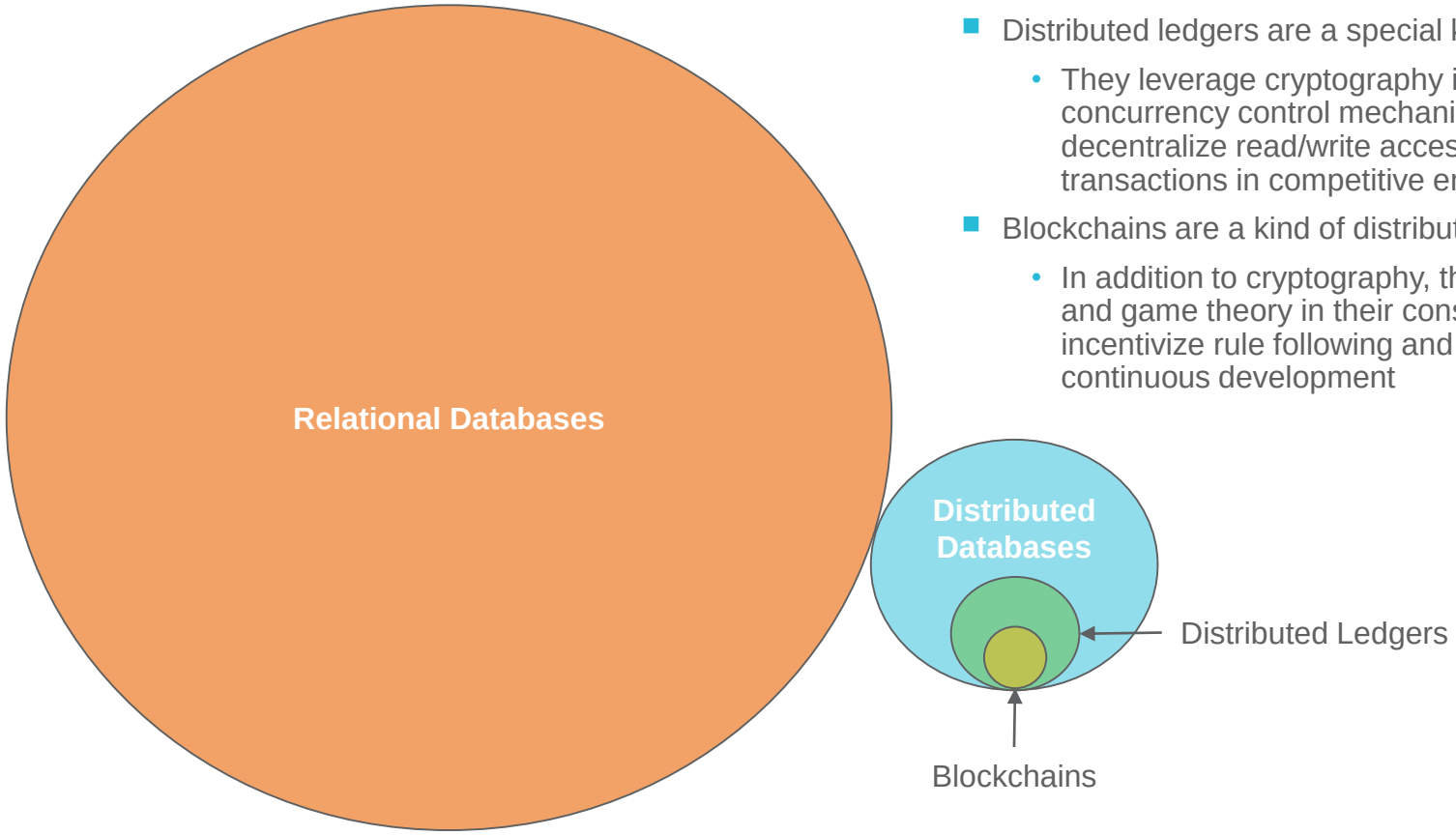
SOURCE: CoinDesk

What Are Blockchains?

Decentralized Data Structures

Blockchains are kinds of organizationally decentralized databases.

- Traditional relational databases store data in tables where it is then accessed using SQL queries (think Microsoft Access or SQL Server). These centrally managed databases comprise more than 90% of the market in terms of revenue
- The remaining 10% of the market is comprised of distributed databases, which are stored across networks for the purpose of distributing risk and leveraging the simultaneous computing power of multiple processors (think BitTorrent)
  - To ensure data integrity, these databases employ consensus mechanisms and concurrency controls such as locking and/or timestamping



- Distributed ledgers are a special kind of distributed database
  - They leverage cryptography in their consensus and concurrency control mechanisms, which allows them to decentralize read/write access, ensure privacy, and secure transactions in competitive environments
- Blockchains are a kind of distributed ledger
  - In addition to cryptography, they leverage cryptoeconomics and game theory in their consensus mechanism to incentivize rule following and ensure the platform's continuous development

SOURCE: Blockchain technology – a very special kind of Distributed Database - Sebastien Meunier on Medium

scottmadden
MANAGEMENT CONSULTANTS

Decentralized Data Structures (Cont'd)

While they are organizationally decentralized, blockchains are simultaneously logically centralized.

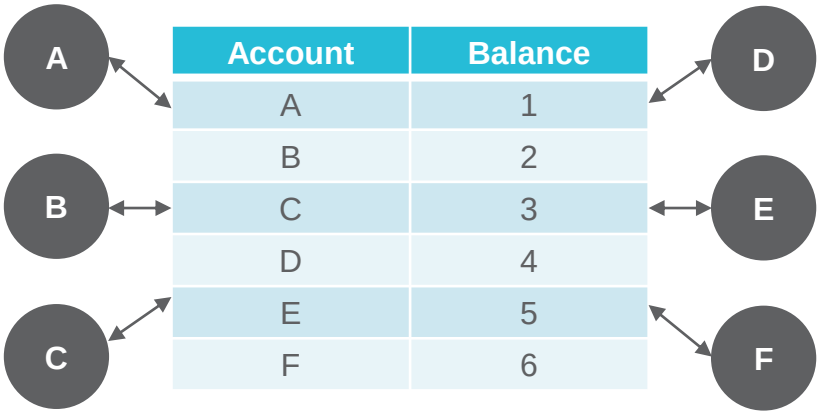
- Blockchains are not controlled by any one entity whether for profit or otherwise, yet they provide the same information to anyone who accesses them
- Until 2008, this wasn't possible at scale, especially in competitive environments lacking trust

	Organizationally Centralized	Organizationally Decentralized
Logically Centralized	Paypal	Blockchains
Logically Decentralized	Excel	Email

The result is a drastically different transaction landscape where peers can now collaboratively maintain a single shared ledger.

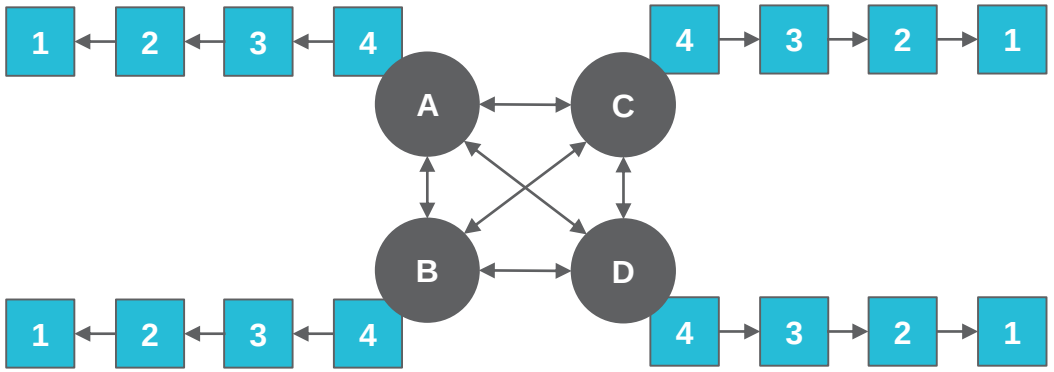
- Unlike currently centralized models, a copy of the blockchain is kept by each peer in the network, and the peers are connected directly to one another without intermediation

Paypal



Account	Balance
A	1
B	2
C	3
D	4
E	5
F	6

Blockchains

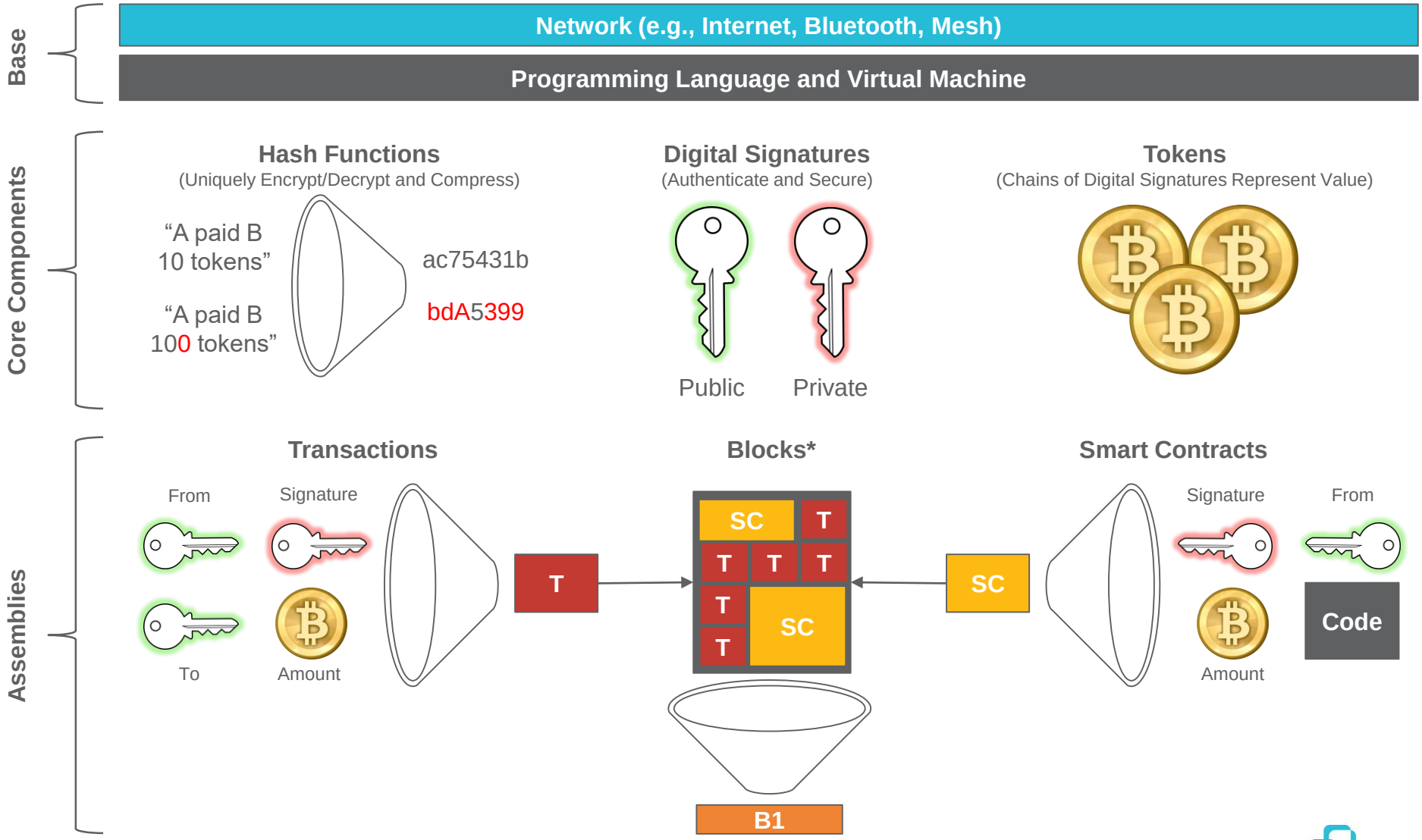


SOURCE: CoinDesk

scottmadden
MANAGEMENT CONSULTANTS

Customizable Ledgers

This new kind of ledger is made of simple, customizable elements that combine to form complex objects and behaviors.



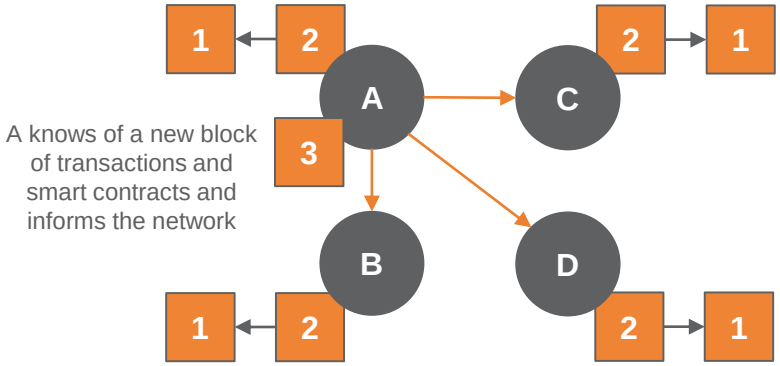
*Transactions and smart contracts are organized in Merkle trees within blocks for purposes of efficiency
SOURCE: CoinDesk; Bitcoin and Cryptocurrency Technologies

scottmadden
MANAGEMENT CONSULTANTS

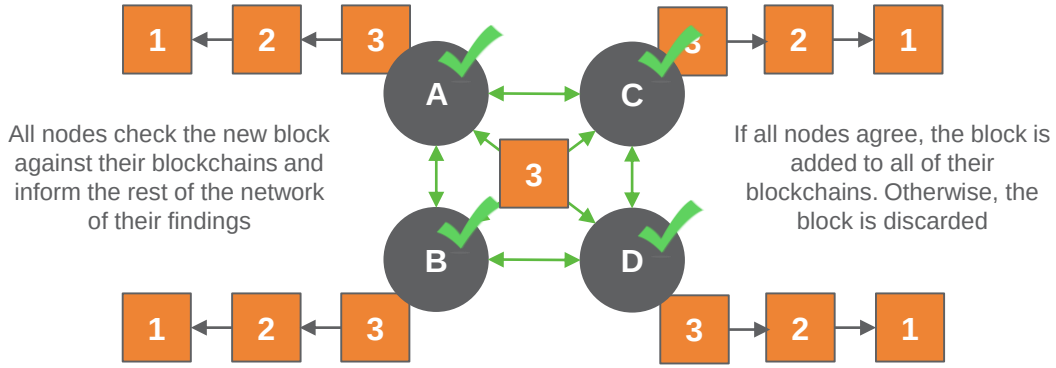
Customizable Ledgers (Cont'd)

Supplementing these elements are two rule-based procedures required to maintain data integrity.

Communication
(Propagation)

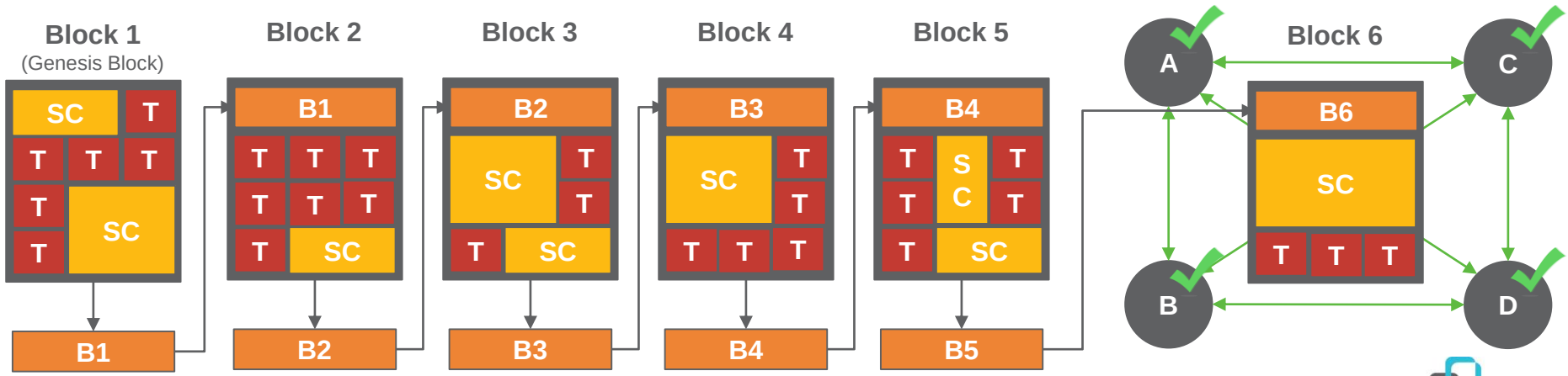


Consensus
(Network Validation)



Blockchains result from the combination of these elements and protocols.

- The major variations between blockchain designs arise from different choices in consensus protocols and token schemes
- Other variations may arise from differences in hash strengths and/or the robustness of the blockchain's programming language



SOURCE: CoinDesk

scottmadden
MANAGEMENT CONSULTANTS

Stores of Value

Just like ordinary ledgers, blockchains can record anything of value while also indicating ownership.

- Identities: contracts that encode the notion of identifying a unique individual actor
- Assets: contracts that model ownership over a particular amount of a class of "stuff"
- Data: contracts that ascribe information to other entities within the ecosystem or otherwise supply "global" information (e.g., about off-chain externalities)

Combining these primitives allows us to glimpse some of the potential applications for blockchains.

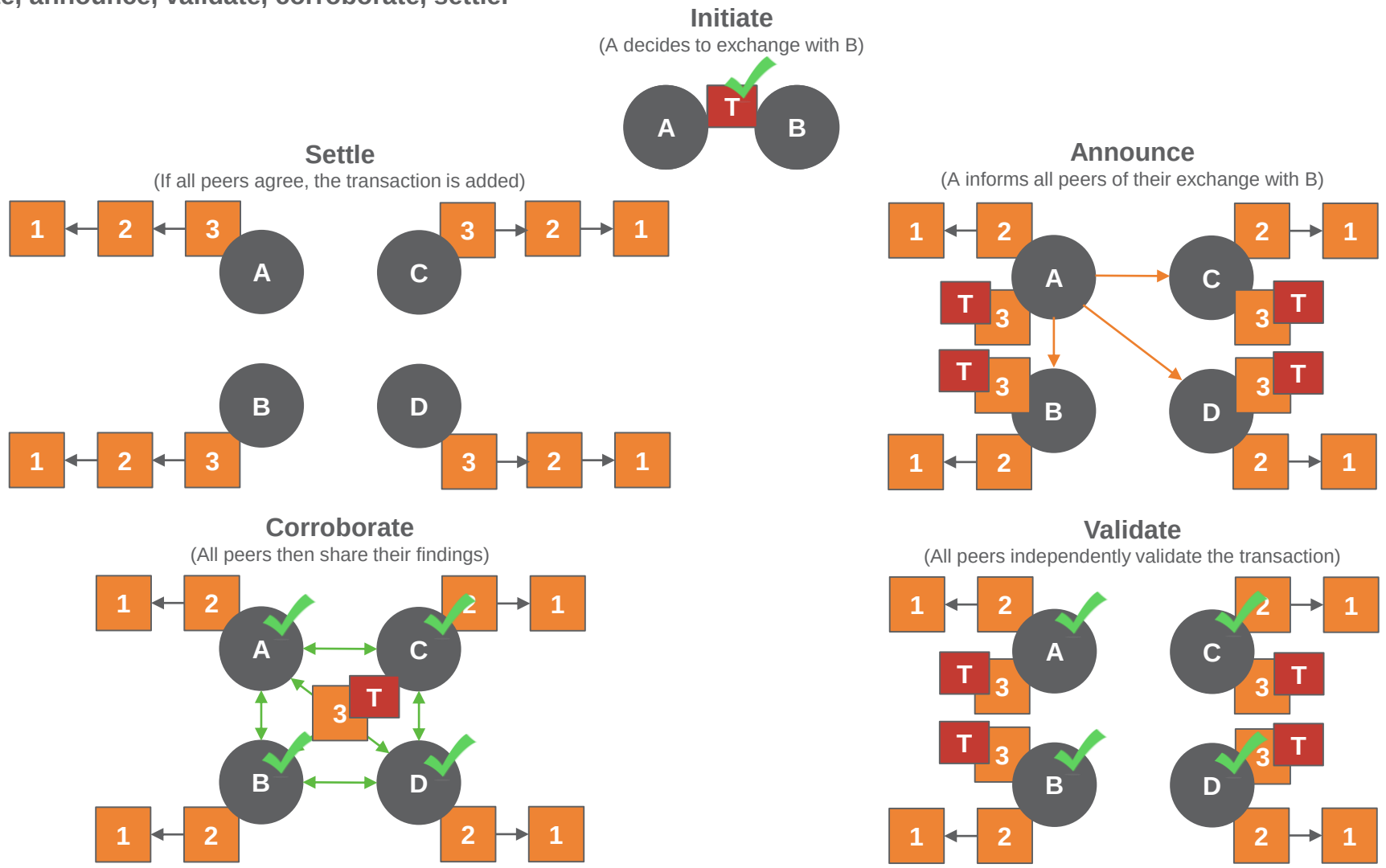
	Identities + Assets	Identities + Data	Assets + Data
First Order Applications	Certification: association without ownership Asset tracking: making fungible assets individual Judged-escrow: combining appeal to an identifiable authority and ownership Bonded identity: assets attached to identities that are controlled externally	Reputation: a means of linearly measuring an entity's virtuosity Badges: non-transferable, non-linear attributes attached to identities Oracles: allow identities to vouch for data	Asset classification Insurance: escrow services where assets are dispersed depending on particular data Gaming: risk-related insurance offerings On-chain currencies: tie to real-world value feeds
Second Order Applications	Court: combine data and reputation to determine truth, and use bonded identities to transfer assets from culprits to victims Transparent supply chain: combine certification and asset tracking	Credit ratings, KYC: higher-order reputation systems Marketplace: reputation plus virtual retail enables on-chain currencies to be exchanged for off-chain assets	Virtual retail: on-chain currencies and assets Trade finance: combine credit ratings, on-chain currencies, and asset tracking to provide cheap, flexible, and reliable liquidity

SOURCE: So Ethereum is Released - Gav Would on Medium

How Do Blockchains Work?

Transaction Life Cycle

From 30,000 feet, the standard operation of a blockchain is straightforward and (can be) nearly instantaneous: (read clockwise) initiate, announce, validate, corroborate, settle.



SOURCE: CoinDesk

scottmadden
MANAGEMENT CONSULTANTS

Cryptoeconomics 101

However, at 15,000 feet, the story isn't as simple…though it is more interesting.

Underlying blockchains is cryptoeconomics, which is a tool used to build systems that have certain desired properties by using cryptography to prove properties that happened in the past while using economic incentives defined inside the system to encourage desired properties to hold into the future.

Cryptography

- Hashes: prove topological order of messages
- Signatures: prove the identity of the sender of a message
- Consensus protocol: proves that a certain amount/kind of energy was exerted
- Time locks and sequential protocols: prove that some amount of time elapsed between messages A and B

Economics

- Tokens: incentivize actors by assigning them units of a protocol-defined cryptocurrency (e.g., block rewards)
- Privileges: incentivize actors by giving them decision-making rights that can be used to extract rent (e.g., transaction fees)
- Rewards: increase actors' token balances or give them privileges if they do something good
- Penalties: Opposite of rewards

Key Concepts

- **Cryptoeconomic security margin**: an amount of money such that you can prove "either a given guarantee is satisfied, or those at fault for violating the guarantee are poorer than they otherwise would have been by at least the given amount of money"
- **Cryptoeconomic proof**: a message signed by an actor that can be interpreted as "I certify that either P is true, or I suffer an economic loss of size X"
- **Faults**: include invalidity, equivocation, ignoring inputs, delaying outputs, and latency

Mining is at the intersection of cryptography and economics.
It is what ensures both security and value and is, therefore, indispensable.

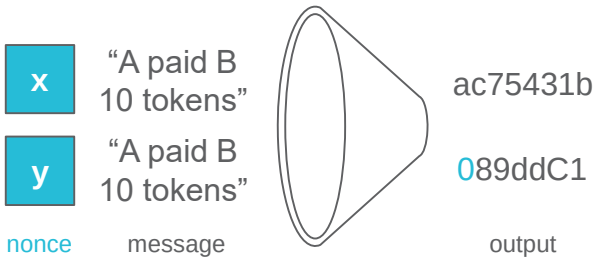
SOURCE: Ethereum Foundation

Mining – Proof of Work

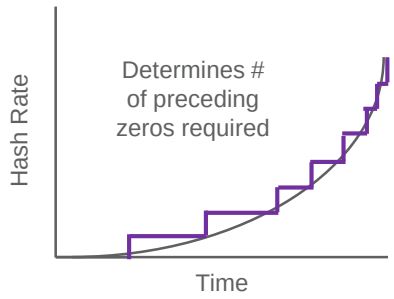
Blockchains leverage mining in their consensus protocols to eliminate the need for trust.

- Blockchains operate in competitive environments. As such, they require an objective means by which all participants can come to the same conclusion about the validity of new transactions and the integrity of all historical transactions
  - They achieve this through a process called mining, which simultaneously validates new and existing blocks while producing new tokens. Once validated, the network is informed of the mined block and proceeds to verify its validity by decrypting its hash
  - The most common mining protocol is known as Proof of Work, which involves exerting computing power to solve a difficult puzzle

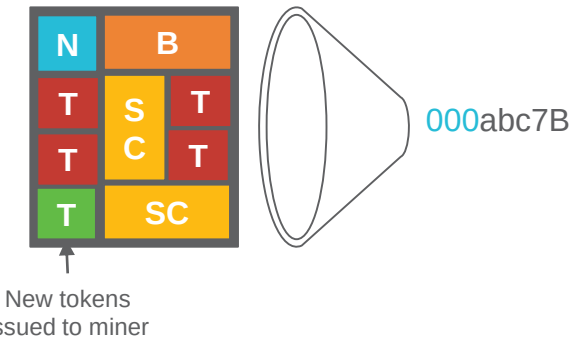
Nonces
(Arbitrary Character Strings Used Once)



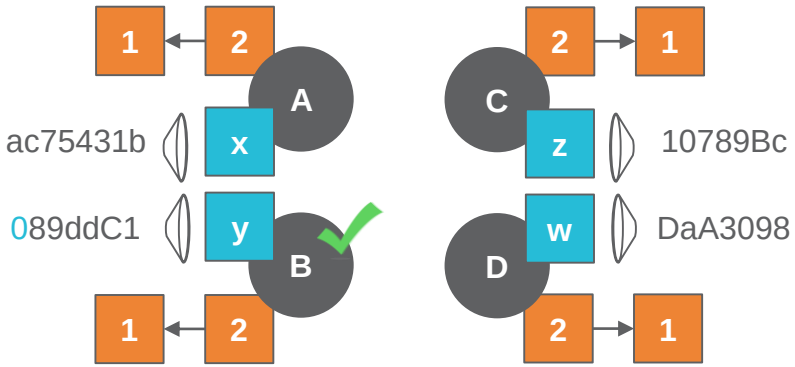
Difficulty Algorithm
(Proportional to Hash Rate)



Blocks
(Include Nonce and Mined Transaction)



Miners
(Nodes Competing to Find Winning Nonce)



Advantages

- Fraud resistant
- Incentivizes rule following
- Mitigates propagation of spam

Limitations

- Energy intensive
- Incentivizes resource centralization
- Limits transactions per second

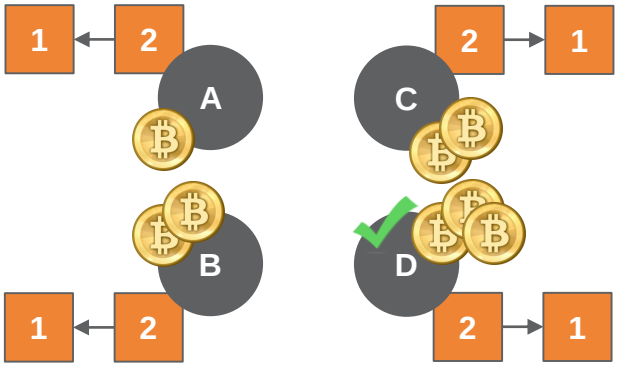
SOURCE: CoinDesk

Mining – Proof of Stake

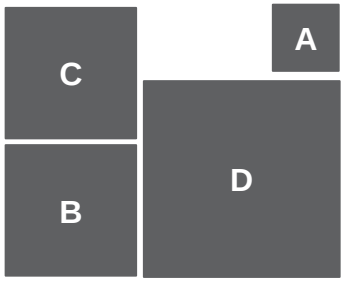
Proof of Stake is the second most common mining protocol used in blockchains.

- In order to eliminate the inefficiencies associated with Proof of Work, Proof of Stake replaces the hardware costs implicit within Proof of Work with token costs that represent the stake of each node in the network
  - By internalizing the previously externalized costs of the network, a lottery algorithm can be employed that selects among a self-nominated group of nodes using a probability distribution proportional to each node's stake; this prevents wasted effort
  - The selected node is the designated miner who informs the rest of the network which block (and contents) should be added
  - Participating miners must store the entire blockchain, and their incentive to tell the truth lies in the transparency of the verification process

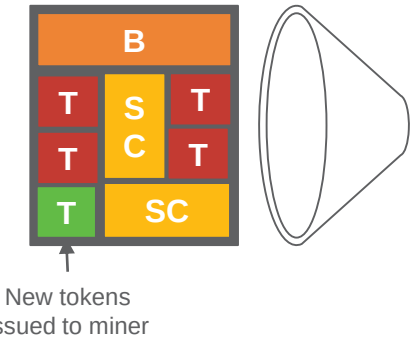
Miners
(Self-Nominated Nodes Compete to be Selected)



Lottery Algorithm
(Probability Proportional to Stake)



Blocks
(Include Mined Transaction)



398abc7B

Advantages

- Minimally energy intensive
- Incentivizes rule following; penalties
- Increases transactions per second

Limitations

- "Rich get richer"
- Enables propagation of spam

SOURCE: CoinDesk

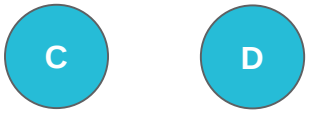
Practical Byzantine Fault Tolerance

Distributed ledgers do not employ mining, but instead rely on a subset of trusted validator nodes to achieve consensus.

- Instead of mining, which involves monetary incentives to ensure rule following and network upkeep, distributed ledgers are typically maintained through external investment via consortia or other similar entities
  - Since all, or most, nodes are known, these networks can select a subset to serve as validators while the rest simply introduce and execute transactions and/or smart contracts
  - A common consensus protocol in these networks is known as Practical Byzantine Fault Tolerance (PBFT)

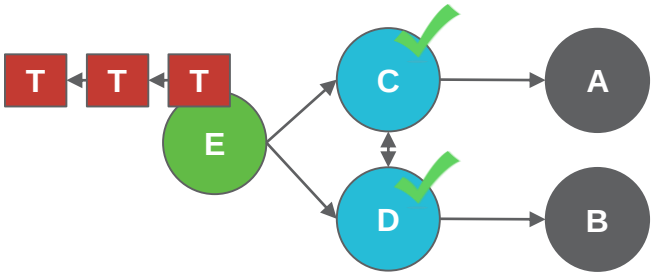
Non-Validating Peers
(Ordinary Nodes Participating in the Network)

Validating Peers
(Special Nodes Participating in the Network)



Validating Leader
(Nominated Validating Peer)

PBFT Consensus
(Validating Leader orders the transactions, which are then voted on by the Validating Peers and disseminated to the Non-Validating Peers)



Advantages

- Fraud resistant
- Private, with known participants
- Speed and efficiency

Limitations

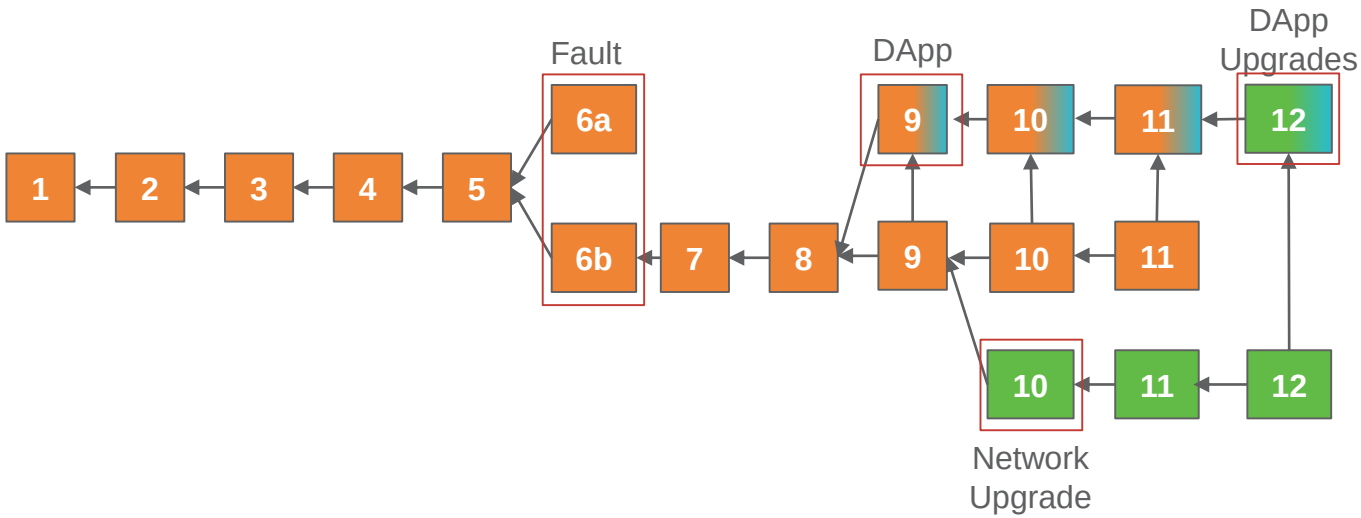
- Relative centralization
- Limited internal incentive to validate
- Mutable

SOURCE: CoinDesk

Forking

When consensus can't be reached, the network induces a fork in the blockchain. These forks are usually ephemeral, since it is in the best interest of the network to maintain a single chain of truth.

- Forks are most commonly resolved in accordance with the consensus protocol, which requires blocks to be added to the longest existing chain that each node is aware of
- On occasion, forks are produced intentionally. This can happen for a number of reasons:
  - A soft fork is one in which a backwards-compatible upgrade is introduced by certain nodes and not others
    - These forks can be used to gradually update the entire network; however, they can also be employed to introduce a new distributed application that runs parallel to the main blockchain and which is intentionally maintained
    - The benefits of soft forks include interoperability with the main blockchain and the ability to customize microeconomic exchanges
  - A hard fork, on the other hand, is one in which an upgrade is introduced that is not backwards-compatible. It is effectively restarting the blockchain
    - These are very rare and typically require 95% or more of the network to adopt before becoming effective



SOURCE: CoinDesk

Current State

Current State

Foundational Applications

As a foundational technology with immense disruptive potential, it is important to understand when and where blockchains should and should not be considered in place of traditional solutions.

1. Bridging Data Silos

- Blockchains enable peers to record and access data using a single shared source
- This can bring substantial efficiencies to systems connecting multiple organizations while retaining privacy and security
- Note: blockchains are most beneficial when allowed to experience network effects. Thus, implementations with limited potential for these effects should be considered carefully

2. Disintermediating Markets

- Markets are made complex by the addition of costly intermediaries that facilitate transactions on behalf of participants
- Blockchains can employ smart contracts that automate the function of intermediaries and simplify markets
- Note: blockchains will not necessarily eliminate intermediaries, but blockchains will significantly impact their value propositions. To stay competitive, traditional intermediaries will have to develop new peer-focused products and services

3. Securing Information

- Unlike centralized alternatives, the redundant storage of the blockchain on each node in its network provides security from targeted attacks while providing an always-on capability like that of the internet
- Moreover, a blockchain's cryptoeconomic architecture ensures immutability and privacy, making it an efficient medium to store valuable, personal information
- Note: blockchains can also be used to store public information and ensure data integrity over time

Blockchains are best applied in environments where communication is flawed, trust is priced at a premium, and data integrity is highly desirable.

SOURCE: CoinDesk

Current State

Commercialization: IBM vs. Microsoft vs. R3

Three very different approaches to commercialization have arisen, each attempting to provide privacy and scalability. However, much like the internet, industries will naturally shift to fewer, interoperable blockchains – a single version of the truth.

IBM

"Blockchain-as-a-Service"

- A suite of cloud services to help clients create and manage blockchain networks
- Based on and almost exclusively supports Hyperledger Fabric's codebase

Hyperledger

- Founding member; direct control over codebase
- Developing private DApps on top of a private distributed ledger using open-source code
- Consensus at the ledger level

Microsoft

"Blockchain-as-a-Service"

- Cloud modules designed to allow developers to quickly create blockchain environments in Azure
- Supports more than 26 blockchains, with preference for the Ethereum blockchain

Enterprise Ethereum Alliance

- Founding member; no direct control over codebase
- Developing private DApps on top of a public blockchain using open-source code
- Consensus at the ledger level

R

"Design-Build; Blockchain-Inspired"

- "Financial innovation firm" leading a consortium of more than 80 of the world's largest financial institutions and regulators
- Designs and produces DLT-inspired solutions for global finance markets

Corda

- Sole developer; direct control over codebase
- Automating legal agreements between identifiable parties on a decentralized database platform using open-source code
- Consensus at the transaction level

SOURCE: http://www.coindesk.com/ibm-vs-microsoft-two-tech-giants-two-blockchain-visions/

scottmadden
MANAGEMENT CONSULTANTS

Technical Developments: The Cutting Edge

As an immature technology, blockchains are still under intense technical development, with private investment driving innovation alongside a pious community of true believers.

- The largest issues being discussed publicly are the same as those being addressed privately: scalability and privacy
  - Proof-of-Stake
    - Virtualizes the mining process, solving wasted electricity and mitigating centralization risks
  - Economic Finality
    - CAP theorem: in the event of a partition, you can have either consistency or availability, not both
    - Solution: availability-favoring base layer, with a consistency-favoring "finality gadget" layered on top of it
      - "Finality gadget": allow users to place a stake on certain histories (analogous to reverse mining); critical mass achieved ensures economic finality
      - Makes hard forks/rollbacks impractical while enabling lite clients
  - Sharding
    - Solves scalability challenges via an architecture in which nodes from a global validator set are randomly assigned to specific "shards," where each shard processes transactions in different parts of the global state in parallel, thereby ensuring work is distributed across nodes rather than being done by everyone
  - Zero-Knowledge Proofs
    - If you encrypt all transactions, how do validators know which ones are valid?
    - Make a cryptographic string that validators can inspect and say to themselves with probabilistic confidence: "no one could have come up with this string if they didn't know a secret key which signed a transaction that obeys all the rules AND *that* transaction is what this encrypted string represents"
    - Brand new scientific discovery

SOURCE: Ethereum Foundation

Next Steps

Putting Distributed Ledger Technologies on the Radar

- Distributed ledger technology (DLT) is garnering increasing attention and interest
- In the financial services industry, companies are hedging against—and leveraging—potential impacts of DLTs on their business
- For other industries, the effects may not be as apparent, but the potential for business model disruption exists for any industry that involves large volumes of transactions and settlements
- Utility and energy companies would be wise to do the following:
  - Monitor developments in the technology and its applications
  - Study potential applications in the energy and utility industries, as well as its limits
  - Influence the development of standards for DLTs in critical infrastructure industries like electric power
  - Incorporate DLTs into strategic planning scenario analyses
- ScottMadden will publish additional research pieces on DLT. We hope this summary and future reports will help keep clients and friends abreast of developments of this potentially powerful technology

The ability to trade electricity could increase substantially the power of customers, as well as grid flexibility and efficiency. Blockchain also could enable customers to easily switch to electricity suppliers with better offers. For example, Electron and Data Communications Company have a platform that enables British customers to sign up to a new seller within a day….

Others argue that a blockchain platform will be a key asset to electric utilities. On the one hand, the technology's ability to circumvent a central point of authority—the utility—suggests individuals and companies will safely and quickly exchange energy services, eliminating a key portion of the utility's business and revenue. On the other hand, a blockchain platform could be a key asset to electric utilities. It could be, as one analyst puts it, "…part of the answer to updating and improving centralized, legacy systems with a distributed hybrid system made up of a patchwork of both large power plants and microgrids powered by distributed energy resources such as solar power."

These analysts admit blockchain will disrupt electricity markets by enabling decentralized power, yet they believe "the established utilities are best placed to evaluate and make strategic bets on blockchain technology's potential applications."

– Energy Post, *How Blockchain Could Upend Power Markets* (May 24, 2017)

Special acknowledgement to ScottMadden Energy Research, and in particular Chris Becker, for its work in preparing this overview.

scottmadden
MANAGEMENT CONSULTANTS

Contact Information

Stuart Pearman

Partner and
Energy Practice Leader

ScottMadden, Inc.
2626 Glenwood Avenue
Suite 480
Raleigh, NC 27608
spearman@scottmadden.com
O: 919-781-4191

scottmadden
MANAGEMENT CONSULTANTS

Smart. Focused. Done Right.

Cristin Lyons

Partner and Grid
Transformation Practice Leader

ScottMadden, Inc.
2626 Glenwood Avenue
Suite 480
Raleigh, NC 27608
cmlyons@scottmadden.com
O: 919-781-4191

scottmadden
MANAGEMENT CONSULTANTS

Smart. Focused. Done Right.

Chris Vlahoplus

Partner and Clean Tech &
Sustainability Practice Leader

ScottMadden, Inc.
2626 Glenwood Avenue
Suite 480
Raleigh, NC 27608
chrisv@scottmadden.com
O: 919-781-4191

scottmadden
MANAGEMENT CONSULTANTS

Smart. Focused. Done Right.

Jon Kerner

Partner

ScottMadden, Inc.
3495 Piedmont Road
Building 10, Suite 805
Atlanta, GA 30305
jkerner@scottmadden.com
O: 404-814-0020

scottmadden
MANAGEMENT CONSULTANTS

Smart. Focused. Done Right.

scottmadden
MANAGEMENT CONSULTANTS