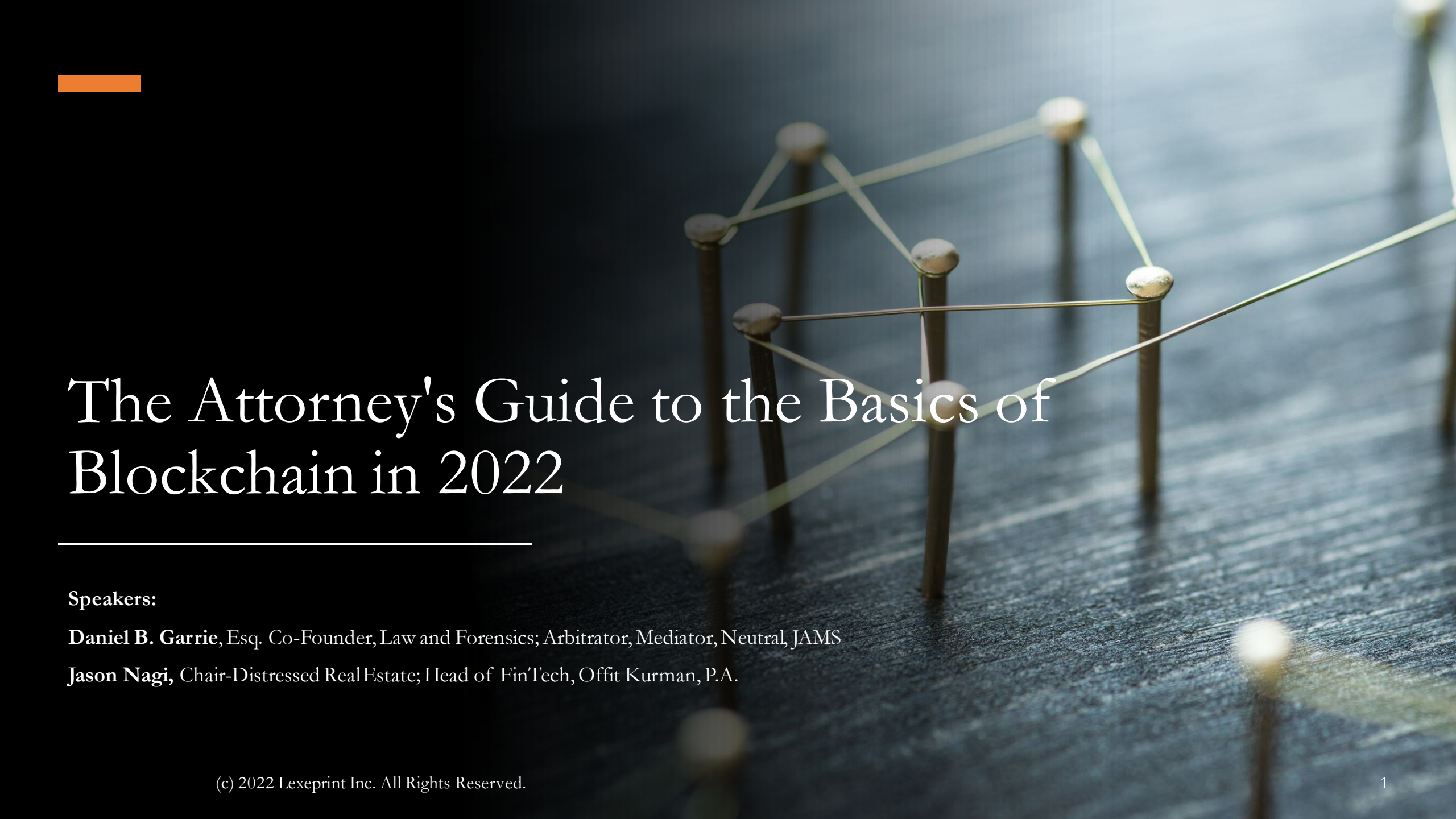


The Attorney's Guide to the Basics of Blockchain in 2022

Speakers:

Daniel B. Garrie, Esq. Co-Founder, Law and Forensics; Arbitrator, Mediator, Neutral, JAMS

Jason Nagi, Chair-Distressed Real Estate; Head of FinTech, Offit Kurman, P.A.

(c) 2022 Lexeprint Inc. All Rights Reserved.

Speakers



Daniel B. Garrie, Esq.
Co-Founder, Law and Forensics;
Mediator, Arbitrator, and e-Discovery
Special Master, JAMS; Partner,
Zeichner, Ellman & Krause LLP



Jason Nagi
Chair-Distressed Real Estate; Head of FinTech
Offit Kurman, P.A.

(c) 2022 Lexeprint Inc. All Rights Reserved.

Disclaimer



This is not legal advice nor should it be considered legal advice.



This presentation and the comments contained therein represent only the personal views of the participants, and do not reflect those of their employers or clients.



This presentation is offered for educational and informational uses only.

(c) 2022 Lexeprint Inc. All Rights Reserved.



Overview of Blockchain Technology

(c) 2022 Lexeprint Inc. All Rights Reserved.



This Photo by Unknown Author is licensed under CC BY-SA-NC

Introduction to Blockchain

- Blockchains are tamper evident and tamper resistant digital ledgers implemented in a distributed fashion (i.e., without a central repository) and usually without a central authority (i.e., a bank, company, or government).
- At their basic level, they enable a community of users to record transactions in a shared ledger within that community, such that under normal operation of the blockchain network no transaction can be changed once published.

(c) 2022 Lexeprint Inc. All Rights Reserved.



What is Blockchain?

- In its simplest form, Blockchain is a data structure on which transactional data which are highly resistant to modification may be stored.
- As a data structure, blockchain is a form of distributed ledger technology that enables data sharing across a network of individual computers.

(c) 2022 Lexeprint Inc. All Rights Reserved.



Lexeprint PUBLISHING GROUP

What is Blockchain?

The main appeal to blockchain technology is twofold:

- all data and transactions that are on the blockchain are nearly impossible to modify or hack
- the data itself is transparent.

(c) 2022 Lexeprint Inc. All Rights Reserved.



Introduction to Blockchain

In 2008, the blockchain idea was combined with several other technologies and computing concepts to create modern cryptocurrencies: electronic cash protected through cryptographic mechanisms instead of a central repository or authority.

The first such blockchain based cryptocurrency was Bitcoin.

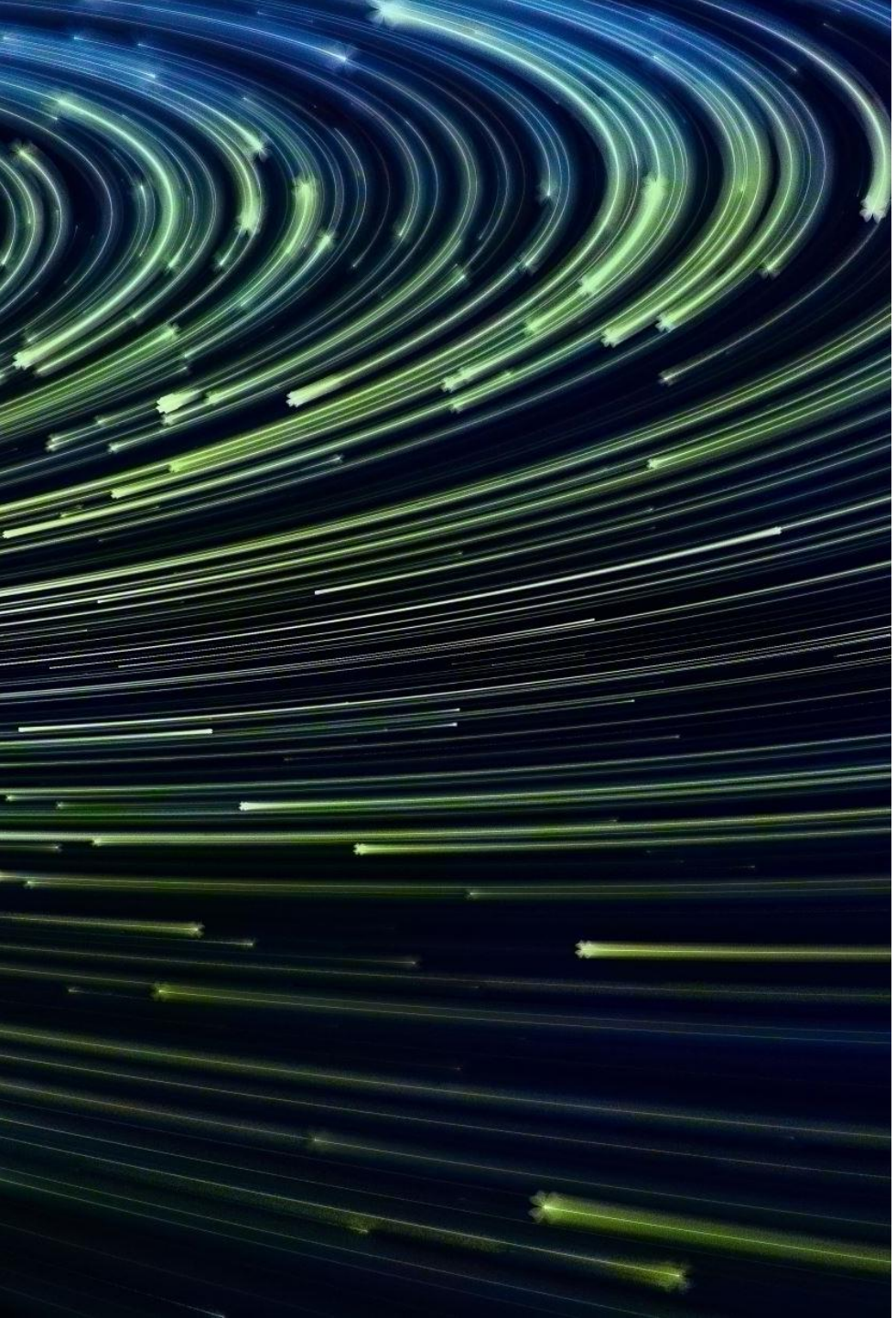
(c) 2022 Lexeprint Inc. All Rights Reserved.



Where is Blockchain Used Today?

(c) 2022 Lexeprint Inc. All Rights Reserved.

This Photo by Unknown Author is licensed under CC BY



Real-World Uses

- Payment Processing and Money Transfers
- Monitor Supply Chains
- Retail Rewards Programs
- Digital IDs
- Data Sharing
- Copyright and Royalty Protection
- Digital Voting
- Immutable Data Backup
- Tracking Prescription Drugs

(c) 2022 Lexeprint Inc. All Rights Reserved.


This Photo by Unknown Author is licensed under CC BY-SA

Lexeprint PUBLISHING GROUP

Real-World Uses

- Tax Regulation and Compliance
- Medical Record Keeping
- Weapons Tracking
- Equity Trading
- Managing IoT Networks
- Expediting Energy Futures Trading and Compliance
- Securing Access to Belongings

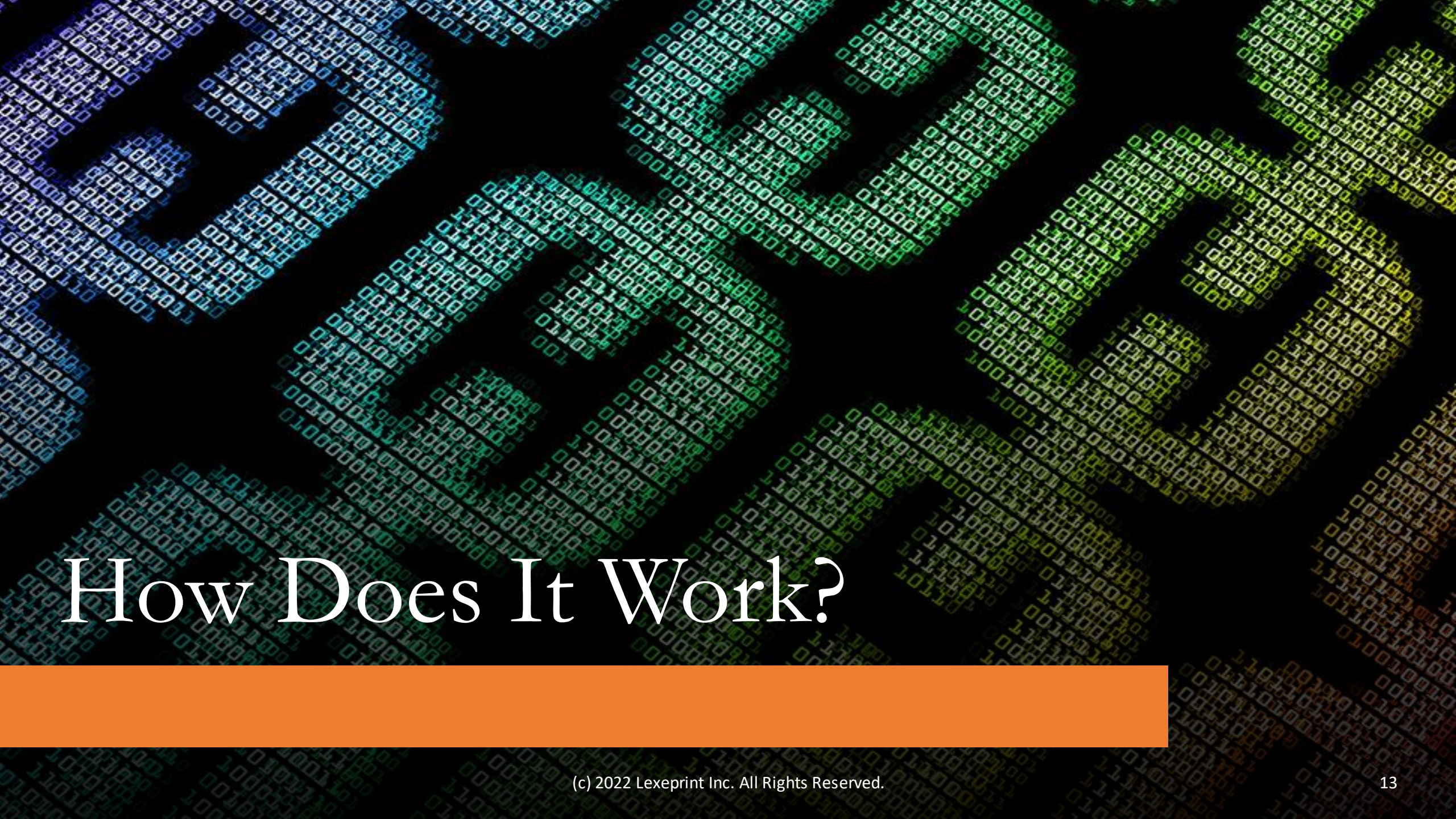
(c) 2022 Lexeprint Inc. All Rights Reserved.



Use Case – International Payments

- Blockchain provides a way to securely and efficiently create a tamper-proof log of sensitive activity. This makes it useful for international payments and money transfers.
- For example, in April 2018, Banco Santander launched the world's first blockchain-based money transfer service, known as "Santander One Pay FX." The service uses Ripple's xCurrent to enable customers to make same-day or next-day international money transfers.
- By automating the entire process on the blockchain, Santander has reduced the number of intermediaries typically required in these transactions, making the process more efficient.

(c) 2022 Lexeprint Inc. All Rights Reserved.



How Does It Work?

(c) 2022 Lexeprint Inc. All Rights Reserved.



How Blockchain Works

- A Blockchain is a type of diary or spreadsheet containing information about transactions.
- An individual block in a blockchain contains the following elements:
  - Block number
  - Data stored in the block
  - Hash of the previous block
  - Hash of the current block

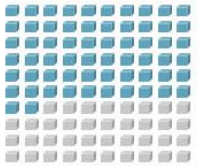
(c) 2022 Lexeprint Inc. All Rights Reserved.

How Blockchain Works

Blockchain Process Steps







P2P Network ⇨ **Communication** ⇨ **Validation** ⇨ **Verification** ⇨ **Confirmation**

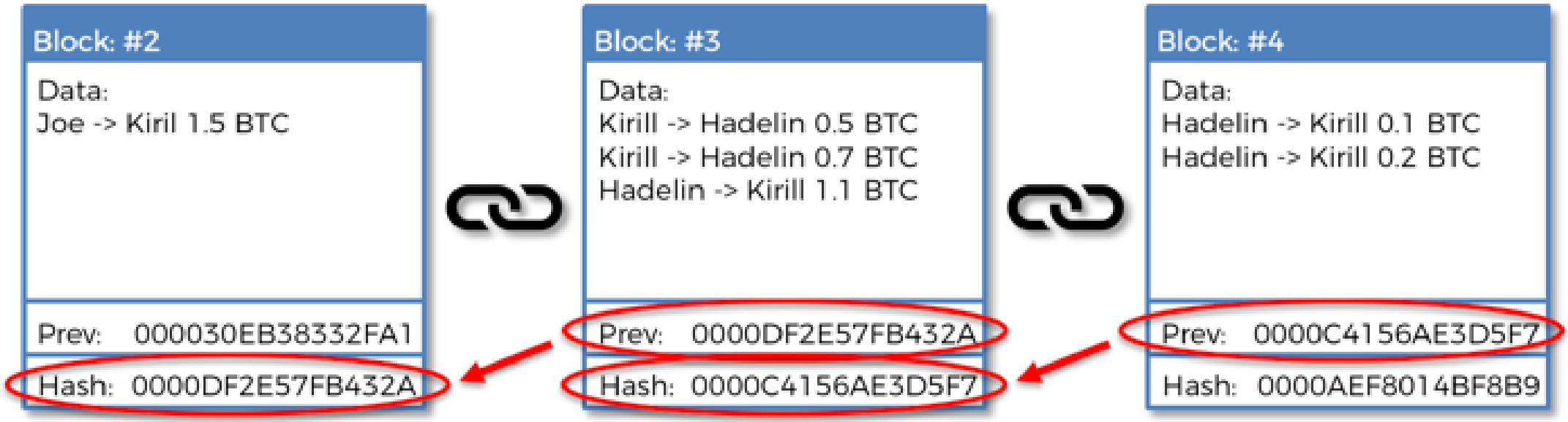
1. Someone in the Peer to Peer network requests a transaction.
2. The requested transaction is broadcast to the P2P network consisting of computers, known as nodes.
3. The network of nodes validates the transaction and the users status using algorithms.

   A verified transaction can involve cryptocurrency, contracts, records or other information.
4. Once verified, the transaction is combined with other transactions to create a new block of data for the ledger.
5. The new block is then added to the existing blockchain, in a way that is permanent and unalterable.

   The transaction is complete.

(c) 2022 Lexeprint Inc. All Rights Reserved.

Implementation – Individual Blocks



(c) 2022 Lexeprint Inc. All Rights Reserved.

Permission vs. Permissionless

Permission Blockchain	Permissionless Blockchain
Require permission to join and participate in consensus	No permission required to join and interact
Governance Structure	Decentralized
Private Transactions	Transparent network
Authentication process	Immutability
Scalable Network	Harder to scale

(c) 2022 Lexeprint Inc. All Rights Reserved.



Validation Methods

- All blockchain networks require a consensus mechanism to validate every new block added to the chain.
- Consensus mechanisms allow nodes on the blockchain to agree upon the accuracy of each block of transactions before it is added to the chain.
- Proof of Work and Proof of Stake are two of the most used consensus mechanisms in the blockchain industry.

(c) 2022 Lexeprint Inc. All Rights Reserved.



Proof of Work vs Proof of Stake

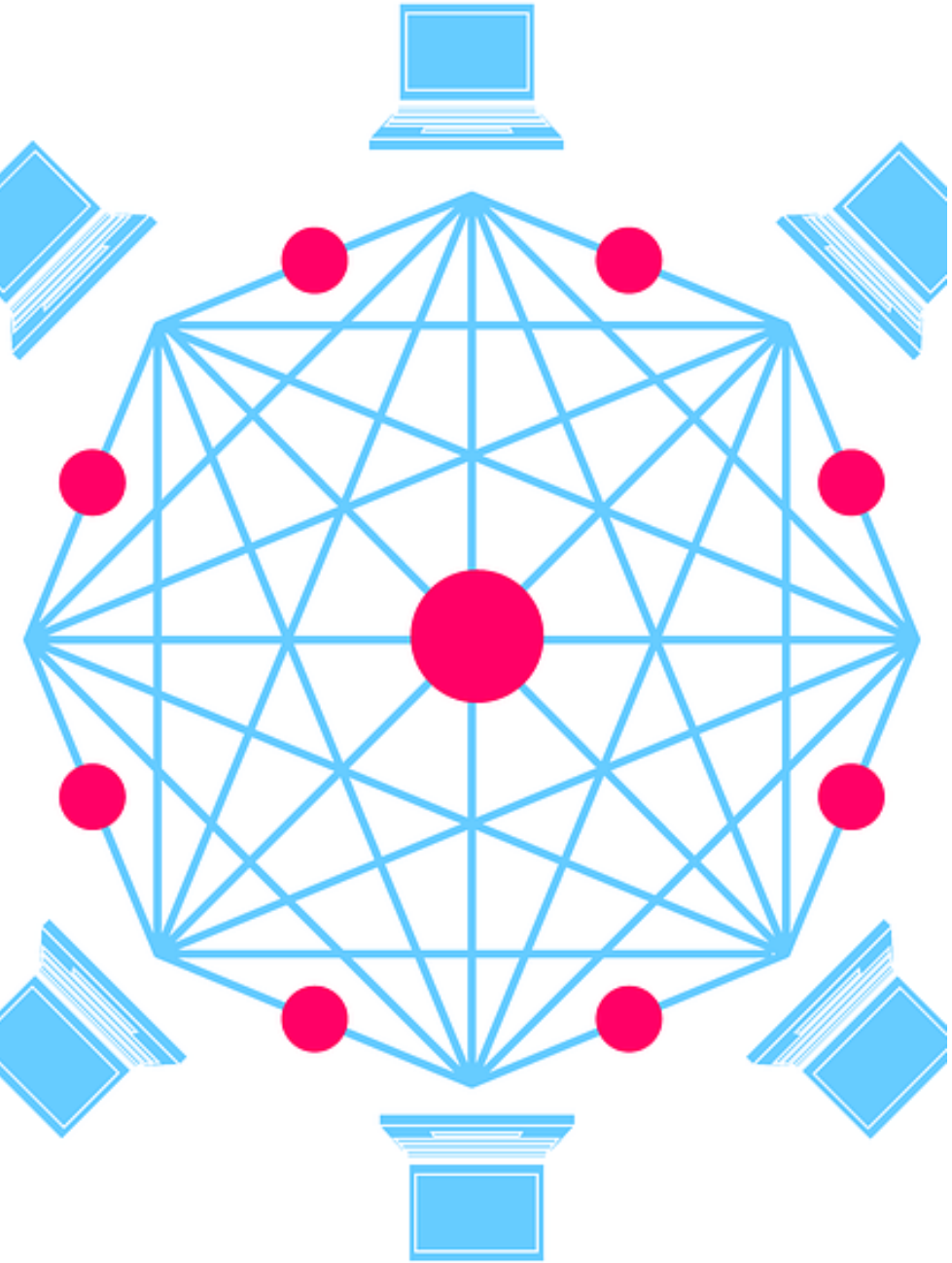
Proof of work	**Proof of Stake**
Participating nodes are called miners.	Participating nodes are called validators or forgers.
Mining Produced new coins.	No new coins are formed.
Miners receive block rewards.	Validators receive transaction fees.
Huge energy consumption.	Low to moderate energy consumption.
Computational power determines the mining capacity.	The stake in the network depends on the validating capacity.

(c) 2022 Lexeprint Inc. All Rights Reserved.



What Makes It Unique?

(c) 2022 Lexeprint Inc. All Rights Reserved.



Decentralizing the System

- Blockchain focuses on decentralizing an entire network. Decentralizing a system refers to an arrangement where there is no single owner of the network.
- Everybody on the network stores a copy of the ledgers and of every block. Using blockchain, the need for middlemen and trust authorities have been eliminated.
- Completing transactions have become easier as this technology allows people to trust each other rather than having them to prove their identities before making any transaction.

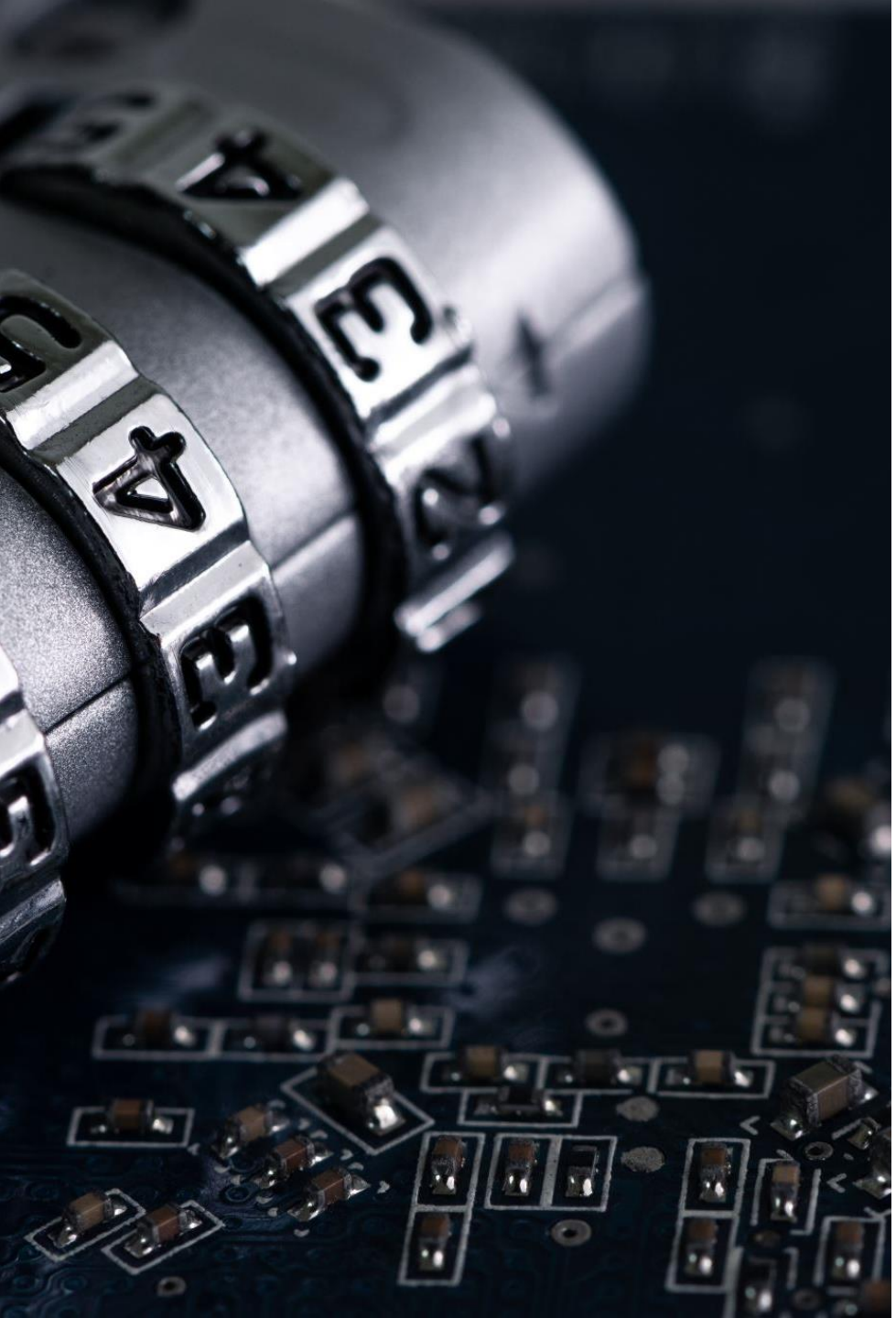
(c) 2022 Lexeprint Inc. All Rights Reserved.



Transparency

- Since blockchain decentralizes the system and enables everybody to arrive on the same network, the ability for people to view transactions becomes easier.
- Blockchain is a technology that increases transparency of transactions, as everybody on the network has a copy of the ledger. This makes the blockchain ledgers tamper-proof.
- Using blockchain technology, people can make transactions from any part of the globe. All they need to do is register themselves on these ledgers. Once registered, they can order anything from any part of the world pay on the blockchain.

(c) 2022 Lexeprint Inc. All Rights Reserved.



Privacy

- Privacy on blockchain is another feature of blockchain that makes it so special. Privacy in blockchain can be maintained as you publish the required data, and still rest assured that your information will not be misused.

- For people to keep their transactions and identity private, they can create private networks where access is limited, and people can choose from a list of entities to be added onto that blockchain network.

(c) 2022 Lexeprint Inc. All Rights Reserved.



Security

- A feature that makes blockchain stand out of the crowd and showcases it as one of the prime-time technologies is its security.
- While making a transaction, your public key is converted into a private key and sent to the person who you want to make a transfer to. The private key sent to the user is a hashed version of the crypto-currency that is to be sent to the receiver. During this transaction, your private key is secure and is not being exchanged with anyone.

(c) 2022 Lexeprint Inc. All Rights Reserved.



Bitcoin Governance Model

- Bitcoin follows a governance model of collaboration of a tradition of open-source software.
- Bitcoin updates its software using the process from the Request for Comments format which was created in 1969.
- Bitcoin utilizes Off-chain Governance. This type of governance operates when all stakeholders agree and make all relevant updates and implementations in unison.
- If a consensus is not reached, the network is split into two chains that run different versions of the software. The successor to the original chain is the chain with the most transactional hashing power.

(c) 2022 Lexeprint Inc. All Rights Reserved.



What is the Relationship Between Blockchain and Cryptocurrency?

(c) 2022 Lexeprint Inc. All Rights Reserved.



Blockchain is the Foundation of Modern Crypto

- Blockchain technology is the foundation of modern cryptocurrencies, so named because of the heavy usage of cryptographic functions. Users utilize public and private keys to digitally sign and securely transact within the system.
- For cryptocurrency based blockchain networks which utilize mining, users may solve puzzles using cryptographic hash functions in hopes of being rewarded with a fixed amount of the cryptocurrency.
- However, blockchain technology may be more broadly applicable than cryptocurrencies.

(c) 2022 Lexeprint Inc. All Rights Reserved.



Blockchain and Cryptocurrency

- Blockchains can enable decentralized platforms which require a cryptocurrency. The blockchain is the technology that serves as the distributed ledger and allows a network to maintain consensus. Distributed consensus enables the network to track transactions and enables the transfer of value and information.
- Cryptocurrencies are the tokens used within these networks to send value and pay for these transactions, or to provide network incentives. Furthermore, you can see them as a tool on the blockchain, in some cases serving as a resource or utility, or even to digitize the ownership of an asset.

(c) 2022 Lexeprint Inc. All Rights Reserved.



Different Types of Tokens

- Cryptocurrency tokens are fungible digital assets. They can be used as mediums of trade inside of the issuing blockchain project's ecosystem.
- Tokens are often referred to as the food that nourishes blockchain-based ecosystems.
- The different types of tokens provide distinctive features on usage.
- Two prevalent token types are: platform and security tokens.

(c) 2022 Lexeprint Inc. All Rights Reserved.



Platform Tokens

- Platform tokens deliver decentralized applications for different uses by using blockchain infrastructures.
- Platform tokens benefit from the blockchains that they build upon.
- These tokens gain enhanced security and the ability to support transactional activity.
- Platform tokens serve gaming and digital collectibles platforms to global advertising and marketplace sectors.

(c) 2022 Lexeprint Inc. All Rights Reserved.



Security Tokens

- As regulatory concerns continued to grow, the term "security token" arose.
- The U.S. Securities and Exchange Commission and other regulatory authorities looked to specify cryptocurrencies using terminology that did not conflict with preexisting legal definitions.
- Security Tokens are direct, on-chain representations of real-world securities.

(c) 2022 Lexeprint Inc. All Rights Reserved.



Current State of the Law and Regulations for Blockchain

(c) 2022 Lexeprint Inc. All Rights Reserved.



Blockchain Regulations in the US

- Few formal rules have been introduced regarding the use of blockchain and cryptocurrencies in the US.
- Most of the regulatory discussion surrounding blockchain has been at the agency level, including the Department of Treasury, Securities and Exchange Commission (SEC), Federal Trade Commission (FTC), Internal Revenue Service (IRS) and Financial Crimes Enforcement Network (FinCEN) — all of which hold different definitions of "cryptocurrency," as well as their stances on how regulation should be applied.

(c) 2022 Lexeprint Inc. All Rights Reserved.



Blockchain Regulations in the US

- While FinCEN does not consider cryptocurrency to be legal tender, it does consider exchanges as money transmitters subject to their jurisdiction.
- Meanwhile, the IRS has begun considering cryptocurrencies property, and has issued tax guidance accordingly.
- Despite interest from these agencies, the federal government has not exercised its constitutional preemptive power to regulate blockchain to the exclusion of states (as it generally does with financial regulation), thereby leaving individual states free to introduce their own rules and regulations.

(c) 2022 Lexeprint Inc. All Rights Reserved.



The Anti-Money Laundering Act of 2020

- On January 1, 2021, Congress enacted the 2021 National Defense Authorization Act (NDAA), which included significant reforms to the U.S. anti-money laundering (AML) regime.
- The NDAA includes the Anti-Money Laundering Act of 2020 (AML Act) and, within the AML Act, the Corporate Transparency Act (CTA).
- The Act also calls for FinCEN to work closely with regulatory and national security agencies, and law enforcement to identify risks and priorities and provide valuable feedback to our industry partners.

(c) 2022 Lexeprint Inc. All Rights Reserved.



Questions?

(c) 2022 Lexeprint Inc. All Rights Reserved.

Contact Us



Daniel Garrie
Email: daniel@lawandforensics.com
URL: www.lawandforensics.com



Rachel Dooley
Email: rsjdooley@gmail.com
URL: https://www.mckinsey.com/



Jason Nagi
Email: jason.nagi@offitkurman.com
URL: https://www.offitkurman.com/

(c) 2022 Lexeprint Inc. All Rights Reserved.



Daniel B. Garrie, Esq.
Law & Forensics – Co-founder
JAMS – Mediator, Arbitrator, eDiscovery Special Master
Contact:
W: (855) 529-2466
E: daniel@lawandforensics.com
URL: www.lawandforensics.com

LAW & FORENSICS
A Global Legal Engineering Firm

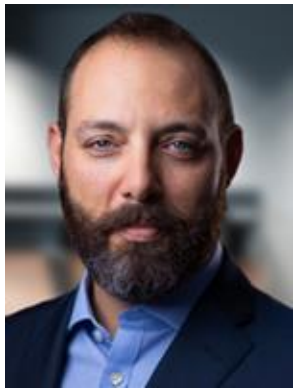
B.A., Computer Science, Brandeis Uni.
M.A., Computer Science Brandies Uni.
J.D., Rutgers School of Law

Daniel Garrie is the Co-Founder of Law & Forensics LLC, Head of Computer Forensics and Cyber Security Practice Groups and has been a dominant voice in the computer forensic and cybersecurity space for over 20 years. Prior to Daniel's legal career, he successfully built and sold several technology start-up companies. Since co-founding Law & Forensics LLC in 2008, Daniel has built it into one of the leading boutique cybersecurity forensic engineering firms in the industry. Daniel has both a Bachelor's and a Master's Degree in computer science from Brandeis University, as well as a J.D. degree from Rutgers Law School. Daniel has led forensic teams in some of the most visible and sensitive cyber incidents in the United States.

Daniel regularly testifies as an e-discovery, cybersecurity and computer forensic expert witness, authoring forensic expert reports on multi-million-dollar disputes. His ability to perform complex investigations and effectively communicate the results to a jury has made him one of the most sought-after experts in the country. His testimony has been pivotal in a number of cases. Since 2008, Daniel has served as a Neutral and Special Master and in 2016, he joined JAMS as one of the organization's youngest Neutrals. At JAMS, Daniel serves as an Arbitrator, Forensic Neutral, and technical Special Master with a focus on cybersecurity, cyrptocurrency, and complex software and technology related disputes.

Daniel is well-published in the cybersecurity space, Editor-in-Chief of the Journal of Law & Cyberwarfare, author of more than 200 articles and books including, "Understanding Software, the Internet, Mobile Computing, and the Cloud. A guide for Judges", published by the Federal Judicial Center. He has been recognized by several United States Supreme Court Justices for his legal scholarship and is a trusted source and a thought leader for cybersecurity articles and opinions, being cited over 500 times to date.

© 2022 Lexeprint Inc. All Rights Reserved.



Jason Nagi
Offit Kurman, P.A. – Chair-Distressed Real Estate; Head of FinTech
Contact:
W: (212) 644-2092
E: jason.nagi@offitkurman.com
URL: https://www.offitkurman.com/

Offit | Kurman®
Attorneys At Law

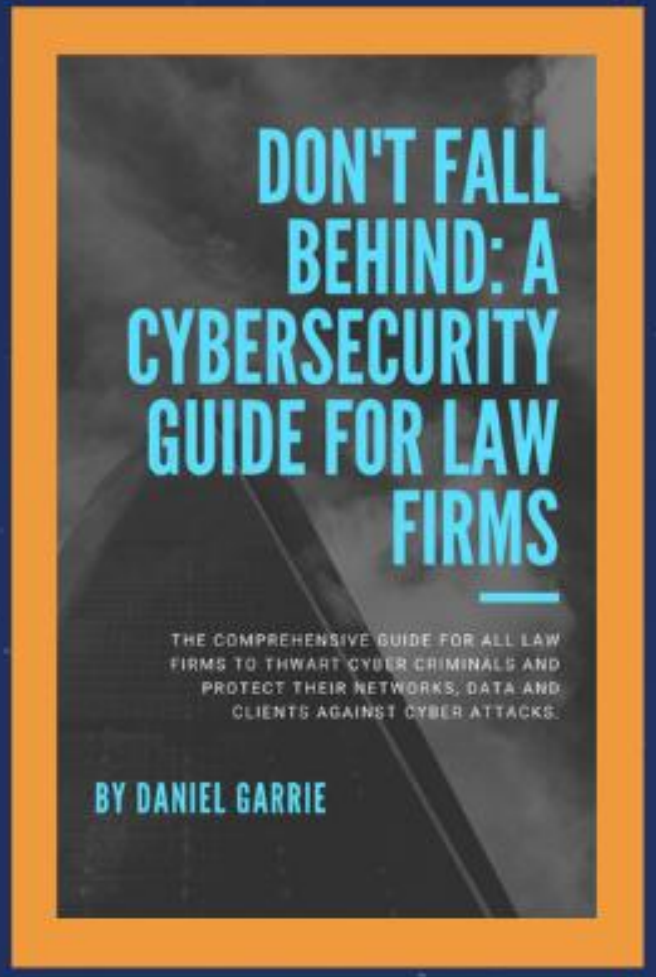
Jason Nagi is a member of Polsinelli's Financial Services Litigation, and FinTech and Regulation practice groups. Jason uses his creditor-focused, finance experience to counsel early stage and mature FinTech companies as well as traditional and non-traditional lenders, in both business ventures and litigation. In addition to appearing before state courts, and U.S. federal district and bankruptcy courts, Jason regularly counsels companies in applying blockchain technology to their respective industries, fundraising efforts, and regulatory issues. Jason advises clients on SEC, CFTC, FinCEN, and state-level MSBs, including the issuance of securitized digital assets.

Jason represents securitized lenders, special servicers, banks, and private lenders in enforcing distressed commercial loans, conducting sales via the Uniform Commercial Code, fraudulent transfer actions, and through every stage of insolvency proceedings. In addition to his experience in Single Asset Real Estate bankruptcy cases, Jason has represented agent banks and majority lenders for syndicated loans, in out-of-court workouts, and both contested and consensual court supervised restructurings. Jason has represented large international corporations, insurance companies, financial institutions, and individual businesses in the federal and state courts in New York and New Jersey.

Jason is a Forbes, Crypto & Blockchain contributor, the host and creator of the CryptoCharacters podcast, has authored numerous articles on FinTech issues, is a frequent speaker at conferences and is a member of the Wall Street Blockchain Alliance advisory board.

(c) 2022 Lexeprint Inc. All Rights Reserved.

A CYBERSECURITY GUIDE FOR LAW FIRMS



"NO ONE IS IMMUNE TO A CYBERSECURITY INCIDENT. EVERY INDUSTRY AND BUSINESS SECTOR—INCLUDING THE LEGAL PROFESSION—IS A TARGET FOR HACKERS AND CYBER CRIMINALS. AS EARLY AS 2009, THE FBI FLAGGED THE LEGAL INDUSTRY AS A GROUP THAT WAS VULNERABLE TO CYBER ATTACKS, ISSUING AN ADVISORY THAT HACKERS WERE INCREASINGLY TARGETING LAW FIRMS."



AVAILABLE ON:

amazonkindle AND PAPERBACK!

Buy Now

How Bitcoin Works

By DAVID FLOYD Updated November 29, 2021

Reviewed by JULIUS MANSA

Fact checked by PETE RATHBURN

How exactly to categorize Bitcoin is a matter of controversy. Is it a type of currency, a store of value, a payment network, or an asset class?

Fortunately, it's easier to define what Bitcoin actually is. It's software and a purely digital phenomenon—a set of protocols and processes.

It is also the most successful of hundreds of attempts to create virtual money through the use of cryptography. Bitcoin has inspired hundreds of imitators, but it remains the largest cryptocurrency by market capitalization, a distinction it has held throughout its decade-plus history.

Like standard currency, Bitcoin is produced and has processes and safeguards in place to prevent fraud and ensure appreciation in its value. The main building blocks of Bitcoin are blockchain, mining, hashes, halving, keys, and wallets. They are discussed in detail below.

(A general note: According to the Bitcoin Foundation, the word "Bitcoin" is capitalized when it refers to the cryptocurrency as an entity, and it is given as "bitcoin" when it refers to a quantity of the currency or the units themselves. Bitcoin is also abbreviated as BTC.[1] Throughout this article, we will alternate between these usages.)

KEY TAKEAWAYS

- **Bitcoin miners run complex computer rigs to solve complicated puzzles in an effort to confirm groups of transactions called blocks.** Upon success, these blocks are added to the blockchain record, and the miners are rewarded with a small number of bitcoins.
- Other participants in the Bitcoin market can buy or sell tokens through cryptocurrency exchanges or peer-to-peer.
- The Bitcoin ledger is protected against fraud via a trustless system; Bitcoin exchanges also work to defend themselves against potential theft, although high-profile thefts have occurred.

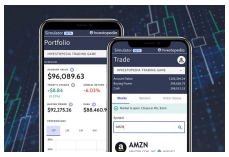


4:24

How to Buy Bitcoin

Investopedia Essentials

SPONSORED



Try the Investopedia Stock Simulator

New to investing? Learn how to trade in real time on our virtual stock simulator. Our platform helps teach you the right strategies for building and maintaining wealth.

The Blockchain

Bitcoin is a network that runs on a protocol known as the blockchain. While it does not mention the word blockchain, a 2008 paper by a person or people calling themselves Satoshi Nakamoto first described the use of a chain of blocks to verify transactions and engender trust in a network. [2]

The blockchain has since evolved into a separate concept, and thousands of blockchains have been created using similar cryptographic techniques. This history can make the nomenclature confusing. Blockchain sometimes refers to the original Bitcoin blockchain. At other times, it refers to blockchain technology in general, or to any other specific blockchain, such as the one that powers Ethereum.

Any given blockchain consists of a single chain of discrete blocks of information, arranged chronologically. In principle, this information could include emails, contracts, land titles, marriage certificates, or bond trades. In theory, any type of contract between two parties can be established on a blockchain as long as both parties agree on the contract. This takes away any need for a third party to be involved in any contract and opens up a world of possibilities including peer-to-peer financial products, such as loans or decentralized savings and checking accounts, wherein banks or any intermediary are irrelevant.

Blockchain's versatility has caught the eye of governments and private corporations; indeed, some analysts believe that blockchain technology will

In Bitcoin's case, the information on the blockchain is mostly transactions. Bitcoin is really just a list. Person A sent X bitcoin to person B, who sent Y bitcoin to person C, etc. By tallying these transactions up, everyone knows where individual users stand. It's important to note that these transactions do not necessarily need to take place between humans.

Bitcoin's blockchain network creates vast possibilities for the Internet of things. In the future, we could see systems in which self-driving taxis or Uber vehicles have their own blockchain wallets. The passenger would send cryptocurrency directly to the car, which would not move until the funds were received. The vehicle would be able to assess when it needs fuel and use its wallet to facilitate a refill.

Another name for a blockchain is a "distributed ledger," which emphasizes the key difference between this technology and a well-kept Word document. Bitcoin's blockchain is distributed, meaning that it is public. Anyone can download it in its entirety or go to any number of sites that parse it. This means that the record is publicly available, but it also means that there are complicated measures in place for updating the blockchain ledger. There is no central authority to keep tabs on all Bitcoin transactions, so the participants themselves do so by creating and verifying "blocks" of transaction data. See the section on mining below for more information.

You can see the status of blocks, and their associated transactions, on sites. Such sites list the address identifier for the transacting parties, dates, the date on which the transaction took place, and the time of the transaction. [3]

The long strings of numbers and letters are addresses, and if you were in law enforcement or just very well informed, you could probably figure out who controlled them. It is a misconception that Bitcoin's network is totally anonymous, although taking certain precautions can make it very hard to link individuals to transactions.

Post-Trust

can't protect it by locking it in a safe or burying it in the woods. In theory, all a thief would need to do to take it from you would be to add a line to the ledger that translates to "you paid me everything you have."

A related worry is double-spending. If a bad actor could spend some bitcoin, then spend it again, confidence in the currency's value would quickly evaporate. To achieve a double-spend, the bad actor would need to make up 51% of the mining power of Bitcoin. The larger the Bitcoin network grows, the less realistic this becomes as the computing power required would be astronomical and extremely expensive.

To further prevent either from happening, you need trust. In this case, the accustomed solution with traditional currency would be to transact through a central, neutral arbiter such as a bank. Bitcoin has made that unnecessary, however. (It is probably no coincidence that Nakamoto's original description was published in October 2008, when trust in banks was at a multigenerational low.) Rather than having a reliable authority to keep the ledger and preside over the network, the Bitcoin network is decentralized. Everyone keeps an eye on everyone else.

No one needs to know or trust anyone in particular in order for the system to operate correctly. Assuming everything is working as intended, the cryptographic protocols ensure that each block of transactions is bolted onto the last in a long, transparent, and immutable chain.

Mining

The process that maintains this trustless public ledger is known as mining. Undergirding the network of Bitcoin users who trade the cryptocurrency among themselves is a network of miners who record these transactions on the blockchain.

Recording a string of transactions is trivial for a modern computer, but mining is difficult because Bitcoin's software makes the process artificially time-

transaction in the blockchain and pile so many trivial transactions on top of it that untangling the fraud would become impossible.

By the same token, it would be easy to insert fraudulent transactions into past blocks. The network would become a sprawling, spammy mess of competing ledgers, and Bitcoin would be worthless.

Combining "proof of work" with other cryptographic techniques was Nakamoto's breakthrough. Bitcoin's software adjusts the difficulty miners face in order to limit the network to a new 1-megabyte block of transactions every 10 minutes. That way, the volume of transactions is digestible. The network has time to vet the new block and the ledger that precedes it, and everyone can reach a consensus about the status quo. Miners do not work to verify transactions by adding blocks to the distributed ledger purely out of a desire to see the Bitcoin network run smoothly; they are compensated for their work as well. We'll take a closer look at mining compensation below.

Halving

As previously mentioned, miners are rewarded with Bitcoin for verifying blocks of transactions. This reward is cut in half every 210,000 blocks mined, or, about every four years. This event is called the halving or "the halvening." The system is built-in as a deflationary one for the rate at which new Bitcoin is released into circulation.

This process is designed so that rewards for Bitcoin mining will continue until about 2140. When all Bitcoin is mined from the code and all halvings are finished, the miners will remain incentivized by fees that they will charge network users. The hope is that healthy competition will keep fees low.

This system drives up Bitcoin's stock-to-flow ratio and lowers its inflation until it is eventually zero. After the third halving that took place on May 11, 2020, the reward for each block mined became 6.25 bitcoins.

Here is a slightly more technical description of how mining works: The network of miners, who are scattered across the globe and not bound to each other by personal or professional ties, receives the latest batch of transaction data. They run the data through a cryptographic algorithm that generates a "hash"—a string of numbers and letters that verifies the information's validity but does not reveal the information itself. (In reality, this ideal vision of decentralized mining is no longer accurate, with industrial-scale mining farms and powerful mining pools forming an oligopoly. More on that below.)

Given the hash 00000000000000000c2c4d562265f272bd55d64f1a7c22ffeb66e15e826ca30, you cannot know what transactions the relevant block (#480504) contains. You can, however, take a bunch of data purporting to be block #480504 and make sure that it hasn't been subject to any tampering. If one number were out of place, no matter how insignificant, the data would generate a totally different hash. For example, if you were to run the Declaration of Independence through a hash calculator, you might get 839f561caa4b466c84e2b4809afe116c76a465ce5da68c3370f5c36bd3f67350. Delete the period after the words "submitted to a candid world," though, and you get 800790e4fd445ca4c5e3092f9884cdcd4cf536f735ca958b93f60f82f23f97c4. This is a completely different hash, although you've only changed one character in the original text.

A hash allows the Bitcoin network to instantly check the validity of a block. It would be incredibly time-consuming to comb through the entire ledger to make sure that the person mining the most recent batch of transactions hasn't tried anything funny. Instead, the previous block's hash appears within the new block. If the most minute detail had been altered in the previous block, that hash would change. Even if the alteration was 20,000 blocks back in the chain, that block's hash would set off a cascade of new hashes and tip off the network.

computing power, pass off fraudulent transactions a few blocks back in the chain. So the Bitcoin protocol requires proof of work.

It does so by throwing miners a curveball: Their hash must be below a certain target. That's why block #480504's hash starts with a long string of zeroes. It's tiny. Because every string of data will generate one and only one hash, the quest for a sufficiently small one involves adding nonces ("numbers used once") to the end of the data. So, a miner will run [thedata]. If the hash is too big, she will try again. [thedata]1. Still too big. [thedata]2.
Finally, [thedata]93452 yields her a hash beginning with the requisite number of zeroes.

The mined block will be broadcast to the network to receive confirmations, which take another hour or so, although occasionally much longer, to process. (Again, this description is simplified. Blocks are not hashed in their entirety but broken up into more efficient structures called Merkle trees.)

(Minutes, 7-day average)

of one new block every 10 minutes. As of November 2021, the current difficulty is around 22.465 trillion, up from 1 in 2009. As this suggests, it has become significantly more difficult to mine Bitcoin since the cryptocurrency launched a decade ago.[4]

Mining is intensive, requiring big, expensive rigs and a lot of electricity to power them. And it's competitive. There's no telling what nonce will work, so the goal is to plow through them as quickly as possible.

Early on, miners recognized that they could improve their chances of success by combining into mining pools, sharing computing power, and divvying the rewards up among themselves. Even when multiple miners split these rewards, there is still ample incentive to pursue them. Every time a new block is mined, the successful miner receives a bunch of newly created bitcoins. At first, it was 50, but then it halved to 25, and then it became 12.5. The fourth halving in bitcoin's history occurred on May 11, 2020, and now the reward is set at 6.25.

mined, and miners will depend solely on fees to maintain the network. When Bitcoin was launched, it was planned that the total supply of the cryptocurrency would be 21 million tokens. [5]

The fact that miners have organized themselves into pools worries some. If a pool exceeds 50% of the network's mining power, its members could potentially spend coins, reverse the transactions, and spend them again. They could also block others' transactions. Simply put, this pool of miners would have the power to overwhelm the distributed nature of the system, verifying fraudulent transactions by virtue of the majority power it would hold.

That could spell the end of Bitcoin, but even a so-called 51% attack would probably not enable the bad actors to reverse old transactions because the proof of work requirement makes that process so labor-intensive. To go back and alter the blockchain, a pool would need to control such a large majority of the network that it would probably be pointless. When you control the whole currency, with whom can you trade?

A 51% attack is a financially suicidal proposition from the miners' perspective. When GHash.io, a mining pool, reached 51% of the network's computing power in 2014, it voluntarily promised to not exceed 39.99% of the Bitcoin hash rate in order to maintain confidence in the cryptocurrency's value. Other actors, such as governments, might find the idea of such an attack interesting, though. But again, the sheer size of Bitcoin's network would make this overwhelmingly expensive, even for a world power.

Another source of concern related to miners is the practical tendency to concentrate in parts of the world where electricity is cheap, such as China, or, following a Chinese crackdown in early 2018, Quebec. Bitcoin mining consumes massive amounts of electricity, and this has led some governments to curtail access to power or designate special rates for Bitcoin miners. This, coupled with the Chinese government's repeated attempts to crack down on mining systems located in that country, has led to a dispersion of miners across the globe. As of

Bitcoin Transactions

For most individuals participating in the Bitcoin network, the ins and outs of the blockchain, hash rates, and mining are not particularly relevant. Outside of the mining community, Bitcoin owners usually purchase their cryptocurrency supply through a Bitcoin exchange. These are online platforms that facilitate transactions of Bitcoin and, often, other digital currencies.

> **Important:** El Salvador made Bitcoin legal tender on June 9, 2021. It is the first country to do so. The cryptocurrency can be used for any transaction where the business can accept it. The U.S. dollar continues to be El Salvador's primary currency.[7]

Bitcoin exchanges such as Coinbase bring together market participants from around the world to buy and sell cryptocurrencies. These exchanges have been both increasingly popular (as Bitcoin's popularity itself has grown in recent years) and fraught with regulatory, legal, and security challenges. With governments around the world viewing cryptocurrencies in various ways—as currency, as an asset class, or any number of other classifications—the regulations governing the buying and selling of bitcoins are complex and constantly shifting.

Perhaps even more important for Bitcoin exchange participants than the threat of changing regulatory oversight, however, is that of theft and other criminal activity. Although the Bitcoin network itself has largely been secure throughout its history, individual exchanges are not necessarily the same. Many thefts have targeted high-profile cryptocurrency exchanges, often resulting in the loss of millions of dollars worth of tokens.

The most famous exchange theft is likely from Mt. Gox, which dominated the Bitcoin transaction space up through 2014. Early in that year, the platform announced the probable theft of roughly 850,000 BTC worth close to $450 million at the time.[8] Mt. Gox filed for bankruptcy and shuttered its doors;[9] to

Keys and Wallets

For these reasons, it's understandable that Bitcoin traders and owners will want to take any possible security measures to protect their holdings. To do so, they utilize keys and wallets.

Bitcoin ownership essentially boils down to two numbers, a public key and a private key. A rough analogy is a username (public key) and a password (private key). A hash of the public key called an address is the one displayed on the blockchain. Using the hash provides an extra layer of security.

To receive bitcoins, it's enough for the sender to know your address. The public key is derived from the private key, which you need to send bitcoins to another address. The system makes it easy to receive money but requires verification of identity to send it.

To access bitcoins, you use a wallet, which is a set of keys. These can take different forms, from third-party web applications offering insurance and debit cards, to QR codes printed on pieces of paper. The most important distinction is between "hot" wallets, which are connected to the internet and therefore vulnerable to hacking, and "cold" wallets, which are not connected to the internet.

In the Mt. Gox case above, it is believed that most of the BTC stolen were taken from a hot wallet. Still, many users entrust their private keys to cryptocurrency exchanges, which is essentially a bet that those exchanges will have stronger defenses against the possibility of theft than one's own computer would.

The Bottom Line

Bitcoin, the digital currency and payment network, is actually software and a purely digital phenomenon—a set of protocols and processes. The main component of Bitcoin is blockchain, a series of digital blocks that are linked together as a list and maintain records of all transactions occurring in its

transactions.

The Bitcoin network is undergirded by mining operations that confirm and process transactions. Miners receive bitcoin as a reward for their effort, and the number of bitcoin awarded to miners is halved every four years in an event known as halving or halvening.

Cryptocurrency exchanges are also important to making Bitcoin work because they enable ordinary users to purchase or trade bitcoins, thereby increasing the number of transactions on its network. Finally, cryptographic keys and wallets are necessary to access and store bitcoin.

How does Bitcoin work?

The most important element to making Bitcoin work is its blockchain—a series of linked blocks that store a record of all transactions conducted in its network. Other important elements of Bitcoin include cryptographic keys and wallets that are essential for access to the cryptocurrency and processes like halving that induce inflation into its network by reducing the number of bitcoin in existence.

How does blockchain make Bitcoin trustless?

Bitcoin's blockchain is a distributed ledger, a series of linked blocks containing transaction records, that is undergirded by complex mining processes to ensure the integrity of transactions. The blockchain is public, meaning anyone can view transactions occurring on it. In this way, in Bitcoin's blockchain, everyone keeps an eye on everyone else, making it extremely difficult for fraud to occur unless there is large-scale collusion between transacting parties.

How does hashing ensure validity of a block?

A hash enables the Bitcoin network to instantly ascertain the validity of a block by checking for the previous block's hash in a new block. The hash must be below a certain target, making it difficult and time-consuming for bad actors to

How are keys and wallets used in Bitcoin?

There are two types of keys in Bitcoin. A public key is used to identify an address on a blockchain and can be likened to a username. A private key is used to access your bitcoin and can be likened to a password that must not be shared with anyone. A wallet is a set of keys and can take on various forms such as QR codes. There are two types of wallets. A hot wallet is connected to the internet, while a cold wallet is not connected to any network.

Investing in cryptocurrencies and other Initial Coin Offerings ("ICOs") is highly risky and speculative, and this article is not a recommendation by Investopedia or the writer to invest in cryptocurrencies or other ICOs. Since each individual's situation is unique, a qualified professional should always be consulted before making any financial decisions. Investopedia makes no representations or warranties as to the accuracy or timeliness of the information contained herein.

Invest $500, Get $50

SPONSORED

Start your crypto journey off with a little something extra. When you invest $500 in one of eToro's Smart Portfolios, you'll get an extra $50. Plus, you'll be investing in a diverse set of crypto assets based on your investment goals — all in just a few clicks. Explore eToro's Smart Portfolios today.

ARTICLE SOURCES ▼

Take the Next Step to Invest

Advertiser Disclosure

Vanguard Digital Advisor

Optimize your investments with retirement planning and investment management

E*TRADE

Trade stocks, bonds, options, ETFs, & mutual funds, in one easy-to-manage account

Betterment

Automated investing and personalized guidance for any financial goal.

PART

Guic ıide

CURRENTLY READING

How Bitcoin Works

2 of 31

UP NEXT

Why Do Bitcoins Have Value?

3 of 31

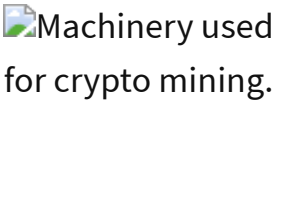
How

4 of 31

Related Articles

BITCOIN

How Does Bitcoin Mining Work?

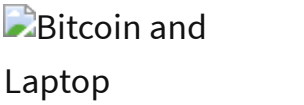


BITCOIN

What Happens to Bitcoin After All 21 Million Are Mined?

BITCOIN

Is Bitcoin Mining Still Profitable?

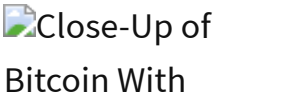


BITCOIN

Bitcoin vs. Bitcoin Cash: What Is the Difference?

BITCOIN

Bitcoin Years Later: Was the Nakamoto White Paper Right?



BITCOIN

Bitcoin's Taproot Upgrade: What You Should Know

Partner Links

25 years' experience as a premium FX provider

Take on the markets w/ confidence. E*TRADE's

Bitcoin Mining

Breaking down everything you need to know about Bitcoin mining, from blockchain and block rewards to proof of work and mining pools. more

What Is ZCash (ZEC)?

ZCash (ZEC) is a decentralized and anonymous payment system. It is an enhanced, transaction-shielded fork of Bitcoin. more

Blockchain Explained

A blockchain is a digitally distributed, decentralized, public ledger that exists across a network. It is most noteworthy in its use with cryptocurrencies and NFTs. more

What Is Double-Spending in a Blockchain?

Double-spending is a potential flaw in cryptocurrency systems that refers to the possibility of a digital currency being spent more than once. more

DigiByte (DGB)

DigiByte (DGB) is a blockchain platform and cryptocurrency. The DigiByte platform processes transactions quickly and uses multiple types of proof of work. more

Bitcoin Definition: How Does Bitcoin Work?

Bitcoin is a digital or virtual currency created in 2009 that uses peer-to-peer technology to facilitate instant payments. more



About Us
Terms of Use
Dictionary
Editorial Policy
Advertise
News
Privacy Policy
Contact Us
Careers
California Privacy Notice



Investopedia is part of the Dotdash Meredith publishing family.

FRESH IDEAS ABOUT BUSINESS IN EMERGING MARKETS EMCompass

www.ifc.org/thoughtleadership NOTE 63 • JAN 2019

Blockchain and Associated Legal Issues for Emerging Markets

By John Salmon and Gordon Myers

Blockchain, or distributed ledger technology (DLT), is a tamper-evident and tamper-resistant digital ledger implemented in a distributed fashion.[1] This emerging technology, which enables direct transactions within a ledger without need for a central authority or trusted intermediary, has the potential to re-engineer economic models and enable the creation of markets and products previously unavailable or unprofitable across emerging markets. However, in considering the potential benefits of blockchain, organizations must also consider the associated risks and how they can be managed.

These risks include jurisdictional challenges, crypto assets, privacy and data protection, double spending, and distributed denial-of-service (DDoS) attacks. Several risks have been identified and overcome at similar innovative leaps in the recent past, including the commercialization of the Internet and cloud computing. It is essential that enterprises understand all risks inherent in blockchain systems, including being able to clearly identify who is accountable and legally responsible.

Blockchain's key characteristics present challenges to the existing legal and regulatory framework. It is comprised of digitally recorded data in "blocks" that are linked together in chronological order in a manner that makes the data difficult to alter once recorded, without the alteration of all subsequent blocks and collusion of a majority of the network.

Each node on the network generally contains a complete copy of the entire ledger, from the first block created—the genesis block—to the most recent one. Each block contains a hash (a fixed length alphanumeric string generated from a string of text) pointer as a link to a previous block, a timestamp, and transaction data. By its nature, distributed ledger technology allows for transactions and data to be recorded and shared across a distributed network of participants without the need for a trusted intermediary. The original instance of blockchain (bitcoin) was to enable peer-to-peer transactions without the requirement for, or cost of, a central party.

Organizations wishing to develop a decentralized application on a blockchain therefore face a new set of risks and issues to manage. Most of these stem from the fact that we live in a world where centralized governance and control is the norm. Accordingly, the vast majority of countries' laws and regulations envision centralized businesses or structures with a singular seat of control and responsibility. Deviating from this arrangement poses a challenge from a legal and regulatory perspective and raises enforcement issues.

This is particularly the case when it comes to regulated sectors such as financial services. In this sector there has traditionally been some form of central counterparty, which often is regulated. Within a particular system or process, that central party is accountable and takes responsibility for the provision of the services to all of the other participants through a contractual framework underpinned by the legal and regulatory structure. An example of this would be the role of a central bank or other institution in clearing and settlement processes.

About the Authors

John Salmon, Partner, Hogan Lovells International LLP, London, UK, and Gordon Myers, Chief Counsel, Legal Department, Technology and Private Equity, IFC, and Co-Chair, Legal and Policy Community, ITS Innovation Lab, World Bank Group. Their emails are john.salmon@hoganlovells.com and gmyers@ifc.org respectively.

This publication may be reused for noncommercial purposes if the source is cited as IFC, a member of the World Bank Group.

IFC International Finance Corporation WORLD BANK GROUP

Creating Markets, Creating Opportunities

BLOCKCHAIN TYPES			Read	Write	Commit	Example
	Open	*Public permissionless*	Open to anyone	Anyone	Anyone*	Bitcoin, Ethereum
		Public permissioned	Open to anyone	Authorized participants	All or a subset of authorized participants	Sovrin
	Closed	*Consortium*	Restricted to an authorized set of participants	Authorized participants	All or a subset of authorized participants	Multiple banks operating a shared ledger
		Private permissioned ("enterprise")	Fully private or restricted to a limited set of authorized nodes	Network operator only	Network operator only	Internal bank ledger shared between parent company and subsidiaries

*Requires significant investment either in mining hardware (proof-of-work model) or cryptocurrency itself (proof-of-stake model)

FIGURE 1 Main types of blockchains segmented by permission model

Source: Hileman, Garrick and Michel Rauchs. 2017. "Global Blockchain Benchmarking Study." Cambridge Centre for Alternative Finance.

However, in many blockchain use cases there is no such centralized party that takes responsibility for the provision of services or controls associated data sets. Instead, each party in the blockchain network holds a copy of the data, rather than relying on a single central party to hold and maintain a master copy. For example, blockchain technology is being used to simplify cross-border payments, removing the need for transfers to pass through multiple parties (with associated charges) before reaching their destination.[2] While such decentralization can bring benefits, it also poses a legal and regulatory challenge if there is no central party that is responsible and can be held accountable.

The key issues that present risks to firms using blockchain, which are explained further below, are: blockchain systems spanning multiple jurisdictions; crypto assets; data protection; privacy compliance; and cyber attacks.

Jurisdictional problems

As the nodes of a decentralized ledger can span multiple locations around the world, it is often difficult to establish which jurisdictions' laws and regulations apply to a given application. There is a risk that transactions performed by an organization could fall under every jurisdiction in which a node in the blockchain network is situated, resulting in an overwhelming number of laws and regulations that might apply to transactions in a blockchain based system.

In a public blockchain system it will be important to consider what law might apply to transactions and consider appropriate risk management that should apply. However, with a permissioned or private system it is easier to create some form of legal framework and internal governance structure that will dictate the governing law that will apply to transactions. In private systems it would also be beneficial to consider some form of agreed dispute resolution process.

Crypto assets

The difficulties of applying the existing regulatory regime can be seen clearly when it comes to the use of crypto assets. We currently see a huge range of opinions from regulators on crypto assets, from outright scepticism and bans in some countries,[3] to more cautious investor warnings from others,[4] while yet other countries have introduced regimes to attract more crypto activity.[5]

These divergences of opinion and the resulting pitfalls are well documented in the example of Initial Coin Offerings, or ICOs. The popularity of selling tokens via ICOs as a means of start-up fundraising has exploded in the last few years. Figures show approximately $21.7 billion has been raised through some 935 ICOs over the period from January to November 2018 alone, dwarfing the amounts raised for blockchain projects via traditional venture capital during the same period.[6] However, given the divergence of regulator opinion on the specific legal implications of a token sale, organizations that fail to consider at the outset whether their token sale may be compliant in the jurisdictions in which they plan to offer tokens may face an uncertain future.

Organizations may also have to ensure that the sale of tokens is limited to buyers in their desired jurisdictions in order to remove the risk of the offer extending to jurisdictions that are more heavily regulated or have outright bans on ICOs. In the United States, the Securities and Exchange Commission (SEC) has expressed concerns that many ICOs are either scams or attempts to raise money without complying with investor protection laws.

This publication may be reused for noncommercial purposes if the source is cited as IFC, a member of the World Bank Group.

IFC International Finance Corporation WORLD BANK GROUP
Creating Markets, Creating Opportunities

Other countries' policy makers and regulators have sought to clarify the position by agreeing that not all ICOs would be required to comply with the same investor protection laws as would be the case with an initial public offering.

This has led to real difficulties for organizations that wish to use tokens in a legitimate way and are committed to complying with the regulatory regime wherever the token is made available. These organizations must deal with varying approaches across different countries, and the position also looks set to change—potentially very significantly—over the next few years.

These problems are particularly stark when one considers the reasons organizations wish to adopt cryptocurrency as part of their infrastructure. The traditional methods of raising capital to fund the growth of a business are debt financing and equity financing. This is clearly seen by both sides as a transaction in which the lender or investor should expect some form of return if the business is successful, but with an appreciation of the risk involved, particularly with early stage businesses.

An organization wishing to sell tokens may be seeking investment, yet it may also be attempting to build a user base through a network effect. If the organization is looking for an investment, it is perfectly reasonable for regulators and policy makers to expect it to comply with the usual investor protection laws; it would not seem equitable for an organization using cryptocurrency to circumvent these laws where the money raised from the tokens is an investment.

However, it is often the case that organizations using a token model want to build a network of users by offering cryptocurrency to use within the particular ecosystem being built. The objective in this case is to encourage people to become users of the organization's services, with the cryptocurrency used to pay for their provision. If the organization proves successful, the value of the token should increase accordingly, as usually there is a finite amount of the new currency sold. In this way, it is the users of the ecosystem who can contribute to and benefit from its success (and popularity), rather than equity investors. These types of tokens are often referred to as utility or consumer tokens, in that they are designed not as an investment but rather a device (or currency) to consume or use a particular service.

In many jurisdictions, regulators have acknowledged that there is a place for such tokens, and that they may not be regulated as an investment. A difficulty arises when organizations wish to sell tokens both to potential users of the system (utility tokens) and to organizations that do not intend to use the prospective service (for example, an investment bank or a venture capital company). Other challenges arise when the purchaser of the token buys many more tokens than the purchaser could possibly use or where there is no usable service at the point when the token is issued. Utility tokens that are sold as investments blur the line between what is regulated and what is not regulated, making it uncertain which regulations an organization must comply with in each jurisdiction in which a token is offered for sale.

These issues, together with the lack of a consistent global regulatory environment, can make it very challenging for those organizations that wish to benefit from the creation of their own crypto asset. There are many reasons why such organizations may want to create their own crypto asset, such as the payment and settlement systems example and the benefit of the network effect mentioned above.

Privacy and data protection

The issue of privacy and blockchain technology has been intensely debated. Many practitioners and academic commentators have claimed that blockchain technology is incompatible with privacy laws such as the EU General Data Protection Regulation, or GDPR.[7]

As mentioned above, the original purpose of blockchain was to facilitate peer-to-peer transactions without the need of a central party. In a permissionless public blockchain system, no single party takes responsibility for the availability or security of a particular blockchain network, and all users of the system may have access to the data on the network. These attributes conflict with the thrust of privacy laws, which require the party controlling personal data of an individual to safeguard the security and privacy of that data on behalf of the individual or "data subject."

Both a controller (the party that determines the purposes and means of processing particular personal data) and a processor (a party responsible for processing personal data on behalf of a controller, such as an outsourced service provider) have distinct obligations under the GDPR, making it important to determine whether a party qualifies as a controller or a processor when processing personal data. With a cloud computing system, typically those uploading personal data to the cloud environment are the controllers and the operator of the cloud system is the processor. This is a key area in which blockchain systems differ. Many blockchain systems are operated by all the users in a peer-to-peer network environment, which makes it difficult to define whether users are controllers or processors. It is necessary to consider to what extent the different participants in the blockchain network are controllers based on their respective activities.

Participants who submit personal data to the blockchain are more likely to be considered controllers under GDPR, as they determine the details of processing, whereas nodes that only process personal data are more likely to be processors, as they simply facilitate the blockchain network's operation. However, this determination is not straightforward, as not all blockchain systems operate in the same way, and there can be different types of participants carrying out various activities.

This publication may be reused for noncommercial purposes if the source is cited as IFC, a member of the World Bank Group.

IFC International Finance Corporation WORLD BANK GROUP
Creating Markets, Creating Opportunities

The nodes in a blockchain system might be compared to autonomous systems on the Internet. Each autonomous system receives packets and routes them autonomously to another node, repeating until the packets reach their destination. The kind of processing that blockchain nodes perform is arguably similar. The only purpose of the nodes is to ensure the integrity of the blockchain and to validate the addition of supplemental blocks. Privacy can be further protected through blockchain systems that use zero-knowledge proofs. This allows nodes in the system to verify transactions without the details of the transaction or the public key, ensuring personal data is not processed by nodes.

In the same way that a cloud service provider may not know what data a customer uploads to its cloud environment, administrators of a blockchain will not necessarily know whether personal data is present on the blockchain. Generic blockchains can be put to a wide variety of uses, and there can be different data and configurations, making it very difficult for the developer to build in privacy protections adapted to the nature of the data processed on the blockchain.

At best, governance rules can regulate users of the blockchain to respect privacy laws when they upload personal data to the blockchain. For private or permissioned blockchains, for particular purposes, governance rules can be much more developed, for example, by prohibiting users from uploading particular types of data to the blockchain.

Transfer of data

There have been debates in the cloud industry about when personal data is "transferred" overseas for privacy law purposes, and blockchain is likely to raise similar questions. For example, if a copy of a hash derived from personal data is made in Singapore, does this mean that data has been "transferred" to Singapore for the purposes of privacy law? In the sense that data may be transferred to a node in any location, data put on a public blockchain is similar to data posted to the public Internet.

The reasoning of the European Court of Justice (ECJ) in the Bodil Lindqvist case may apply to the question of transfer, although this case was in respect of the European Data Protection Directive, which preceded GDPR.[8] The ECJ held that it cannot be presumed that the word "transfer," which is not actually defined in the Directive, was intended to cover the loading by an individual of data onto an Internet page. A similar pragmatic approach is required for data on a blockchain to ensure that it is not "transferred" to every jurisdiction in which a node is present, causing unnecessary breaches of privacy regulations. As there is no single model for blockchain systems, each project will have to be analyzed on its own distinct merits.

Data security on blockchain

Blockchain technology is often referred to as "tamper proof." This is generally because each new digital 'block' containing a record of transactions is connected to all preceding blocks. In order to tamper with any of the records contained in a block, a dishonest participant would need to change all subsequent blocks in the chain to avoid detection.

Given that blockchain is a decentralized ledger, there is no single point of failure that dishonest participants can override. Instead, they would require a huge amount of power to override and alter every node simultaneously. This is especially prominent in public blockchains where there can be any number of nodes existing anywhere in the world. Blockchain therefore presents a lower risk of attack than with centralized systems, in which key servers can be targeted and altered without trace.

Blockchain also uses advanced public key cryptography to secure its data, which relies on users having two cryptographically matched keys. When someone wants to send a user a file, they send the file to a user's public key. The file can then only be opened by the user's correlating private key. Together these features make blockchain a very secure method of recording data. There is relatively low risk of data tampering or data being intercepted compared to traditional methods of transfer and storage, making blockchain a risk management system.

Risk of cyber-attack

Despite the high level of security that blockchain systems provide to the data recorded on them, there are some key cybersecurity risks that remain.

The unique challenge to decentralized systems, particularly public blockchains, is that data input can be from any number of nodes, meaning there is a risk of tampering at each node. The benefit of using a 'tamper proof' technology is negated if the information stored on the ledger is compromised to begin with. This type of attack is not aimed at the blockchain itself, but at external systems such as cryptocurrency wallets. There is a risk that individuals might target the data input point (rather than the ledger itself), leading to the dissemination of inaccurate information. Users operating on the blockchain would then unknowingly rely on misleading or false information. A 15-year-old boy from the United Kingdom proved this attack possible by developing a proof-of-concept code that allowed backdoor access into hardware wallets sold by Ledger.[9] Using this approach, it would be possible to change wallet destinations and amounts of payments. An attacker could divert payments to his own account while making it appear to be the intended destination, ensuring the attack is undetectable to verifying nodes.

Another way data on a blockchain can be compromised is by a targeted brute force attack on certain nodes. In some blockchain networks, a concentrated number of nodes carry

IFC International Finance Corporation WORLD BANK GROUP
Creating Markets, Creating Opportunities
This publication may be reused for noncommercial purposes if the source is cited as IFC, a member of the World Bank Group.

out almost all of the processing. If someone were to identify and attack the nodes covering the required consensus level, the chain could be compromised. However, such an attack requires an enormous amount of computing power.

In some systems an attack would only need to control more than half of the computing power of all nodes. Such attacks are more likely to be successful if the attacker specifically attacks the nodes with the highest computing power in which most transactions are concentrated.

Double spending and DDoS attack

Double spending attacks occur when the same currency unit is assigned to multiple users, enabling them to use the same coin simultaneously.

A distributed denial-of-service, or DDoS, attack is a type of cyber-attack in which a perpetrator attempts to render a service unavailable to its users by overwhelming its bandwidth, often by flooding it with traffic. Blockchain systems are less susceptible to these kinds of attacks than are traditional centralized systems, given the lower numbers of potential points of failure and ability to include denial of service prevention. However, where ledgers are concentrated on a few high-performing nodes, the likelihood of a successful DDoS attack is increased.

Smart contracts

Smart contracts are self-executing software code that runs on a blockchain. They are not in themselves contracts, and often are not particularly smart. Contract law will likely apply to the underlying transactions between the parties using smart contracts, assuming that the arrangement between the participants otherwise fulfils the requirements for contract formation.

The code in the smart contract defines the terms of an agreement on an "if" and "else" basis and then automatically enforces those terms if and when the specific criteria programmed into the code are met. For example, the execution of a smart contract can be verified by the network of users on a blockchain system, removing the requirement of a trusted third-party intermediary. Smart contracts therefore have the potential to reduce costs in areas that typically rely on an intermediary today, such as clearing and settlement.

As demonstrated in 2016 by the hack of the Decentralized Autonomous Organization (DAO) public blockchain, it is possible to target smart contracts that are run on blockchain systems.[10] In the instance of DAO, the hacker was able to move approximately $50 million in investor funds to a sub-contract that the hacker controlled. This type of attack is less likely to occur in private blockchain systems due to the number of users that have access to the smart contract; however, features should be built into the smart contract to ensure that any hack can be corrected retroactively.

As mentioned above, traditional contract law may well apply to the underlying transactions embodied by smart contracts and, as such, the same liability issues apply to smart contracts. Software developers could therefore be liable for poorly written software code that results in a loss for their client, either through exploitation such as the DAO hack, or as a result of the code executing in a way not intended by the parties to the transaction.

Governance Impacts

Accountability

In relation to decentralized systems, a key question for regulators is who should be held accountable for breaches of law and regulation. This is similar to the problem of determining accountability on the Internet before the emergence of blockchain. Accountability of the various parties carrying out relevant activities on the Internet has been a vexing problem since its inception. Prior to the Internet, information and other content, such as music and video, could only be published through existing publishers with an established distribution network. Where there were legal issues about content, for instance issues with copyright infringement and defamation, the publisher was clearly accountable.

In the case of Google Spain v AEPD, the Court of Justice of the European Union (CJEU) ruled that a search engine could be held accountable for the protection of personal data in respect of third party websites accessible through its service.[11] It was emphasized in this case that the search engine's activities could be clearly distinguished from those of the original publisher of the data. The harm to the data subject was not a result of the publication, but rather from the widespread availability of this information through a search engine.

In a public blockchain system, by contrast, there is no one easily held accountable in the same way as a search engine. In a private blockchain system, where there is clear ownership and responsibility, regulators might expect those running the system to be accountable for data added to the system by all the network users. The system owner could be seen as enabling the distribution of data through the blockchain in a comparable way to a search engine. It would then be the system owner's responsibility to protect this data, despite not publishing the personal data itself. The owner would likely have to put in place a set of operating conditions on the private blockchain that comply with regulations, which all users would in turn agree to comply with.

Taxation challenges

The application of existing tax frameworks to a digitalized economy has posed significant challenges to national and global tax authorities. For example, digital economy concerns are at least partly within the scope of the OECD's Base

This publication may be reused for noncommercial purposes if the source is cited as IFC, a member of the World Bank Group.

IFC International Finance Corporation WORLD BANK GROUP
Creating Markets, Creating Opportunities

Erosion and Profit Shifting (BEPS) concerns. In some cases, governments have suggested that broad-based "virtual" profit allocation rules, rather than existing permanent establishment concepts, should apply. India has introduced an "equalisation levy" on payments made to certain non-resident on-line service providers.[12] The European Union has considered similar measures. Over the longer run, a "virtual permanent establishment" concept is envisaged.

These ongoing discussions may have significant implications for blockchain and distributed ledger technology platforms. For example, it seems evident that cryptocurrency transactions will be taxed as assets, that is, on a capital gains basis, without application of VAT. However, issuances of utility tokens, for example, to employees, may be more appropriately taxed as income. Similarly, for policy reasons, government authorities may prefer to defer revenue recognition until disposition, or provision of the underlying services, as is the case in Israel. These are complex matters that, even within a BEPS framework, may promote competitive tax practices that other authorities may view with concern.

In the case of non-cryptocurrency platforms, BEPS-type concerns may well influence industry and governance structures in unintended ways. For example, industry DLT platforms for supply chain management may tend towards centralization, so that they are owned and nominally governed (consistent with BEPS limitations) from low-tax jurisdictions. Similarly, "smart contracts" more efficiently executed on-chain, may be moved off-line to centralized operations to ensure favorable tax treatment of ledger transactions. This solution may achieve compliance, however, at the cost of the efficiencies and certainty argued to arise from using a blockchain-only architecture.

Regulators working with the industry

To allow the financial industry to enjoy the full benefits of blockchain technology, it will be necessary for regulators to work with the industry to ensure that compliance with regulation can be achieved while still allowing blockchain technology to be used to maximum potential. In some jurisdictions, regulators may be required to move away from the use of detailed and prescriptive rules in favor of broadly stated principles that set the standards at which the industry must operate. This would allow regulations to be flexible enough to encompass the wide variety of systems that blockchain allows for. Even in these jurisdictions, however, regulators should work closely with stakeholders to ensure that their thinking on acceptable industry practices is transparent. As in Singapore and the United Kingdom, these efforts can support innovation by providing "bright line" certainty to new and non-traditional industry entrants.

One opportunity to adapt regulatory compliance to distributed ledger technology could be the use of regulatory sandboxes. These provide the ability to test services with real customers in a controlled environment without incurring regulatory consequences. Regulators can gain an understanding of the function of the blockchain systems and cooperate with the industry to identify and develop methods for compliance. This would help regulators develop a level of regulation that encourages and enables innovation while ensuring adequate protection for users—and would encourage development of technology solutions (such as electronic identification, authentication, and trust services that mitigate, for example, anti-money laundering and ultimate beneficial ownership concerns). One challenge of regulatory sandboxes is ensuring they are attractive to start-ups. Sandboxes should encourage innovation and allow for start-ups to grow, rather than merely offering value for the regulator.

Another opportunity to adapt regulatory compliance may lie in careful application of existing regulatory principles to the blockchain environment. For example, regulators will inevitably favor more centralized blockchain and DLT platforms that provide a "home" for regulatory supervision. Alternatively, in decentralized systems, they may take the view that all participants are liable for compliance issues. A more nuanced approach also may be possible. For example, in relation to regulation of privacy issues in unpermissioned systems, France recently took the view that only active participants—those actively inputting data into the system, and not mere "nodes" or "miners" providing verification of transactions to the platform—are responsible as data controllers.[13] This approach may more effectively balance the public interest in large-scale "trustless" systems, by ensuring meaningful accountability for privacy and personal data practices.

Finally, tax issues may continue to challenge the industry. Absent global agreement on "digital economy" principles, one can surmise a fragmented global tax environment, consisting on one hand of aggressively low-tax environments targeted at attracting "producers," and on the other hand, aggressively extraterritorial jurisdictions, targeted at realizing offshore income they believe has been derived from "consumption" in their home territory. Such a tax environment is uncertain for innovation, generating risky tax structures and deterring investors.

Meeting governance objectives

Blockchain system designers may seek to incentivize good behavior by participants in order to meet governance objectives and reduce the risk of non-compliance with regulation by the blockchain network. This may be done by setting rules that ultimately induce the right behavior. Bitcoin, for example, incentivizes miners to verify legitimate transactions by rewarding them with bitcoins. Bitcoin mining is difficult and inefficient by design, making it costly for any node that deviates from the correct protocol and fails to receive a reward.

Designers of blockchain systems could ensure compliance with the legal and regulatory framework by building it into

IFC International Finance Corporation WORLD BANK GROUP
Creating Markets, Creating Opportunities
This publication may be reused for noncommercial purposes if the source is cited as IFC, a member of the World Bank Group.

the system. For example, participants could be locked out of the system unless and until they had been through an appropriate anti-money laundering compliance check.

Beyond blockchain and DLT platform design, decentralized systems pose significant governance and capacity challenges for participants and platforms alike. Fortunately, the industry and regulators have coalesced around key principles for digital platforms and outsourced information technology operations, providing a strong basis for risk governance. Key elements include careful management of information assets; board oversight of resilience and business continuity; development of operational risk metrics and integration with robust enterprise risk management capacity; and considered protocols for management of data incidents.

The proposed European Banking Authority outsourcing guidelines for banks in Europe are a good example of how regulators expect banks to manage outsourced risk, whether based on new technologies such as the cloud or on more traditional models. It is inevitable that regulators will expect the same level of risk management, due diligence, and ongoing monitoring of suppliers of blockchain based systems. Where there is no "supplier" as such (as for a public blockchain), regulators may be hard-pressed to establish oversight responsibilities beyond assuring robust diligence, risk governance, and reporting by users.

We can safely assume that regulators will want to ensure that transparency and understanding of smart contracts are embedded into blockchain and DLT applications. We can similarly surmise that legacy entities participating in blockchain and DLT platforms will want to "flow down" their requirements to governed platforms with a single point of accountability. This would suggest at least that even open permissionless systems will require thoughtful user understandings and allocations of liability, perhaps resembling governing organizations for open source software, to attract commercial users. For the immediate future, it may also suggest that use of permissioned and limited applications is more likely.

Two other governance areas will require resolution if the opportunities inherent in open, trustless systems are to fully emerge. First: decentralized autonomous organizations may present an entirely new mechanism for the organization of capital and commercial activity. Yet the structuring of these vehicles—with regard to risk management, minority protections, and transparency—remains an area for research and evolving practice. Second: there are concerns that the lack of a single point of accountability in a blockchain or DLT platform makes that platform an unincorporated joint venture in which all participants are jointly and severally liable for outcomes.

This is partly reflected, for example, in the French GDPR decision discussed earlier. While, as with the French decision, courts may ultimately limit this exposure to active participants and contributors, this will not be the argument made by plaintiffs' counsel. It is possible that some combination of a strict liability regime, together with statutory liability limitations and support of an appropriate insurance product, will be required. However, as in some public permissionless systems, this approach may be problematic when identity is not apparent, making apportioning liability difficult. This is yet another reason why we view entirely pseudonymous systems as unlikely to be acceptable to regulators, at least in regulated or sensitive settings.

A number of recent articles suggest that development of significant, impactful blockchain applications remains several years away. We do not believe this to be the case. At least for permissioned, governed systems, the regulatory and governance principles allowing public and private players to implement and operate these principles, on a risk assessed basis, are in place.

The more significant concern is that the continued relevance of these principles may deter realization of the full range of opportunities inherent in open, trustless systems. **Our discussion suggests that the application of these frameworks effectively requires a point of accountability for governance and liability, or in the alternative, some measure of joint and several liability by all participants.** More radical decentralization may require more interesting "compliance by design" elements, such as digital identifiers and ultimate beneficial ownership verification; agreed risk reporting available to participants and regulators, embedded in the platform's information architectures; and perhaps some form of overarching liability allocation framework, possibly comprising strict liability principles paid from a pool established by participants and supported by insurance and liability limitations.

The alternative position is that—at least in the short term—an accountable intermediary will be required. One option is that industry foundations, similar to those that exist for key open source software and content licenses, can facilitate the transition to more comprehensive decentralization. Another option is that a private sector technology company takes responsibility for the provision of the blockchain system (some of which might be provided in a permissionless way) in the same way that private companies provide open source software. This option may defeat the entire purpose of using a decentralized blockchain system, as it effectively centralizes the platform and requires users to trust that the provider is acting honestly (and will likely require that they pay a fee for the provision of the system). A partially, but perhaps more effectively, decentralized model may include a consortium of private sector providers who share responsibility, cost, and allocation of liability.

Conclusion

It is clear there are a number of important risk management concerns for any organization wishing to adopt blockchain technology. However, we have seen many of these

This publication may be reused for noncommercial purposes if the source is cited as IFC, a member of the World Bank Group.

IFC International Finance Corporation WORLD BANK GROUP

Creating Markets, Creating Opportunities

challenges before in the adoption of the Internet generally, as well as other technologies such as cloud computing. The key is for the organization to truly understand the risks inherent in the system and to ensure that these are adequately managed and mitigated where necessary. The critical remaining issue is that the structure of contractual frameworks and associated regulation was not designed for the decentralized data world of blockchain. In particular, understanding who is accountable and legally responsible is a major challenge. It is clear to us that the adoption of the technology would be treated like any other form of outsourcing. For those wishing to adopt this new technology, there are three potential models to consider:

One. Private or permissioned models where a single party or group of parties takes responsibility for operating the system. This is the easiest path and would be no different from existing outsourcing/cloud arrangements. A node controlled by a regulator could also be included to act as a neutral party.

Two. Public blockchain systems where there is a clear contractual framework between the participants—one which reflects a more "joint venture" approach and which looks to allocate liability and accountability to the parties. This could be accomplished effectively by a kind of end-user license agreement that conditions use of the public platform on adherence; or perhaps even something that feels like an open-ended fund, where anyone can join but there is a clear legal structure and risk allocation. In general, it would seem that this model would have to be implemented on the inception of the system.

Three. Public blockchain systems where an organization takes on the responsibility and liability for running the system. This could be through open source systems such as Hyperledger, which has a core framework in place and the ability for organizations to alter the network according to their needs, grant permissions to those who need it, and keep out those who don't.[14]

It will likely be difficult for any organization that has to ensure effective risk management to consider a purely permissionless blockchain system without some additional protections. Of course, not all organizations have the strict requirements of financial services companies and other organizations in highly regulated sectors. Regardless of the model adopted by those seeking to use blockchain, it is important that regulators remain flexible in their approach to this emerging technology—and avoid viewing it through a lens designed for more traditional, centralized platforms.

ACKNOWLEDGMENTS

The authors would like to thank the following colleagues for their review and suggestions: Leslie Sturtevant, Manager, Practices AMC, Mobilization, Equity, Climate & Trust Funds, Legal, IFC; Andrew Yew, Senior Counsel, Legal, IFC; Rachel Alexandra Halsema, IT Officer, Business Management I, Technology and Innovation, World Bank Group; Baloko Makala, Consultant, Technology and Innovation, Information and Technology Solutions, World Bank Group; and Thomas Rehermann, Senior Economist, Thought Leadership, Economics and Private Sector Development, IFC.

Additional Reports and EM Compass Notes about Blockchain: *Blockchain – Opportunities for Private Enterprises in Emerging Markets* (report), IFC, October 2017; *Blockchain Governance and Regulation as an Enabler for Market Creation in Emerging Markets* (Note 57); *Using Blockchain to Enable Cleaner, Modern Energy Systems in Emerging Markets* (Note 61).

---

1 Yaga, Dylan, Peter Mell, Nik Roby, and Karen Scarfone. 2018. "Blockchain Technology Overview." National Institute of Standards and Technology.

2 Deloitte. 2016. "Blockchain Technology – Speeding Up and Simplifying Cross-Border Payments." Also: Arnold, Martin. 2018. "Ripple and Swift Slug It Out Over Cross-Border Payments." *Financial Times*. June 5.

3 One example is China.

4 Many EU jurisdictions have issued warnings on the use of cryptocurrency but continue to apply existing legal principles.

5 Gibraltar and Malta are examples of countries advocating cryptocurrency. See Gibraltar Finance. 2018. "Token Regulation: Proposals for the Regulation of token Sales, Secondary token Market Platforms, and Investment Services Relating to Tokens." Parliament of Malta, Virtual Financial Assets Act 2018.

6 Figures as of 8 November 2018. https://www.coinschedule.com/stats.html

7 The General Data Protection Regulation (EU) 2016/678.

8 *Bodil Lindqvist v Aklagarkammaren i Jonkoping*, Case C-101/01.

9 See Goodin, Dan. 2018. "A 'tamper-proof' currency wallet just got backdoored by a 15-year-old", arstechnica.com, March 31, 2018. https://arstechnica.com/information-technology/2018/03/a-tamper-proof-currency-wallet-just-got-trivially-backdoored-by-a-15-year-old/

10 https://en.wikipedia.org/wiki/The_DAO_(organization).

11 *Google Spain SL, Google Inc. v Agencia Espanola de Proteccion de Datos (AEPD), Mario Costeja Gonzalez*, Case C-131/12.

12 Indian Government. 2016. "Equalization Levy Rules."

13 CNIL. 2018. "La Blockchain: Quelles Solutions Pour un Usage Responsable en Présence de Données Personnelles?"

14 Corriveau, Adrianna, Deanna Vitale, and Brittany Manchisi. 2018. "Hyperledger Fabric: What You Need to Know about the Framework that Powers IBM Blockchain." *IBM Blog.*

This publication may be reused for noncommercial purposes if the source is cited as IFC, a member of the World Bank Group.

IFC International Finance Corporation WORLD BANK GROUP

Creating Markets, Creating Opportunities