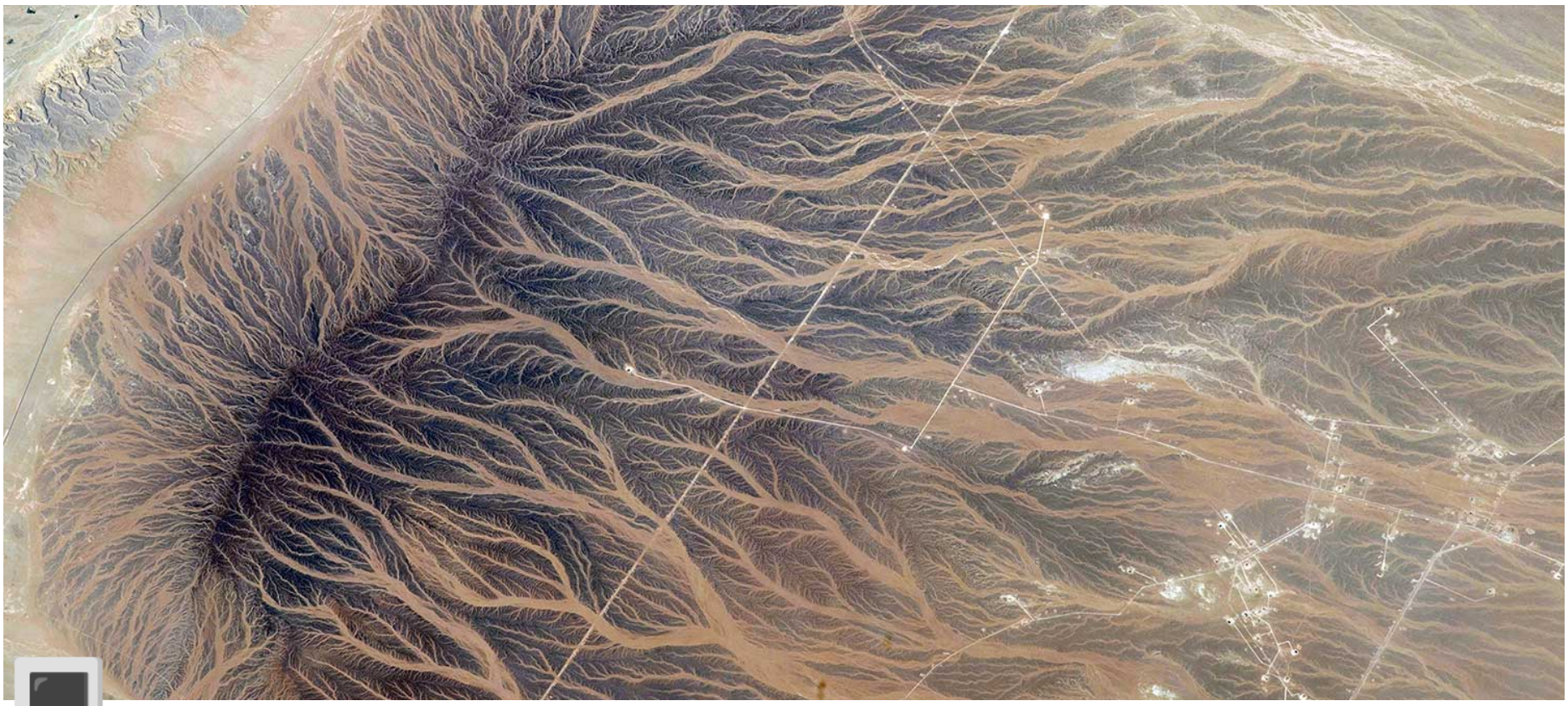


1. Introduction to Blockchain for Financial Services

Abridged by PaddingtonMacro@SPECTRUM CAPITAL LLC.
PC: www.paddintonmacro.com; Mobile: http://m.paddingtonmacro.com

The Internet of Information (1st Era of Internet)

Before Bitcoin (Blockchain) era, internet was designed to move information not things of value - at least not without an intermediary.

1st 4 decade of internet was great:

- reducing cost of searching, collaborating and exchanging information
- lowering the barriers for entry for many new media and entertainment, new forms of retailing and organizing work and new digital ventures
- outsourcing has helped the developing world to join the global economy

Limitations/Problems:

Still need intermediaries like banks and government agencies to establish our identities and to enable us to exchange value, like money online.

- collect our data for commercial gain and for national security
- the cost structure excludes 2.5bn people from the global financial system

It has trouble preserving our **privacy**, establishing our **identities**, and then **including all of us**.

Huge institutions now control what was supposed to be a shared global resource: the internet.

GDP is growing but job growth is pretty much flat. More wealth is created, but also sees greater social inequality.

Internet of Information → Internet of Value

The Internet of Value (2nd Era of Internet)

2008, the collapse of the financial markets, showed that intermediaries were not behaving with integrity and almost brought down the global capital system.

Then, Satoshi Nakamoto's protocol (BTC) was born. Satoshi's protocol uses distributed computations around the world all working on the same problem. It sets up rules to verify the data, exchanges among billions of devices without going through a trusted 3rd party.

With peer-to-peer verification, there's no need for a 3rd party-no need for a mortal, fallible entity to act as "God".

The trust protocol is the basis for more and more distributed ledgers, blockchains.

Big banks and some governments are using blockchains to revolutionize how they store information and conduct transactions：

- faster speed
- lower costs
- greater security
- fewer errors.

A blockchain also **eliminates central points of attack and failure**. None of these reasons requires cryptocurrency.

A blockchain is a specific type of distributed ledger, is public, is open-source code, is a protocol, not a product. The blockchain has heavy duty encryption, using public and private keys (2-key access system).

> *BTC blockchain as an example:*
> *Every 10 minutes, like the heartbeat of the Internet, all transactions conducted on the Bitcoin network are verified, cleared, and stored in a block. The block is linked to the preceding block and to the block before it, creating a chain of blocks. Each block must refer to the preceding block to be valid. The structure permanently timestamps, and stores exchanges of value, and it prevents anyone from altering the ledger. This validation process makes theft impossible by any practical measure. If you wanted to steal a bitcoin, you'd have to rewrite the coins' entire history on the block chain. What's more, you'd have to do it without being detected by millions of other people working on it. Well, that's practically impossible.*

We can program a blockchain to **record virtually everything or anything of value and importance**. It can track anything that we can express in code. What's more, it verifies these records in **near real time**.

Trust in transactions came from acting with integrity.

4 values of integrity:

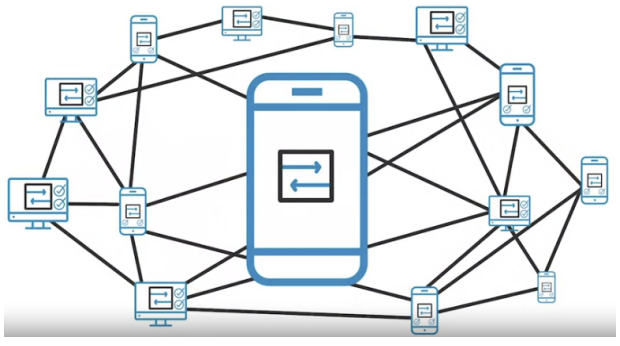
- Honesty
  It’s not only an ethical issue, but also an economic one.
- Consideration
  Trust requires a genuine respect for the interest of the other party. In any transaction, all parties care about the others and will operate in good faith.
- Accountability
  Making clear commitments and sticking with them.
- Transparency
  The transparency and trust built into blockchain will start to rebuild the trust in our institutions.

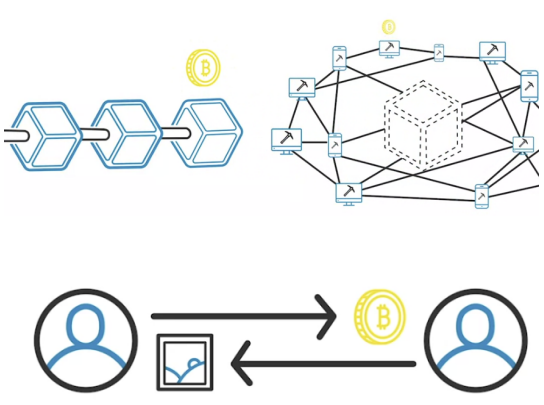
The **smart contracts**, parties will keep their promises automatically.

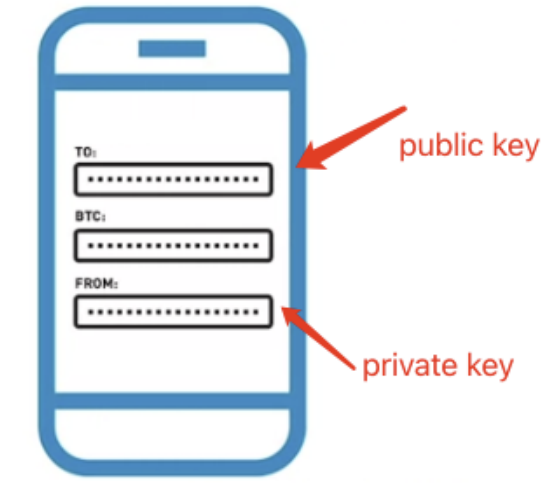
How Blockchain Works

It doesn’t work through powerful intermediaries, it works through the mass collaboration of miners, public key cryptography, clever codes. The parties broadcast the transactions and the network validate the transactions.

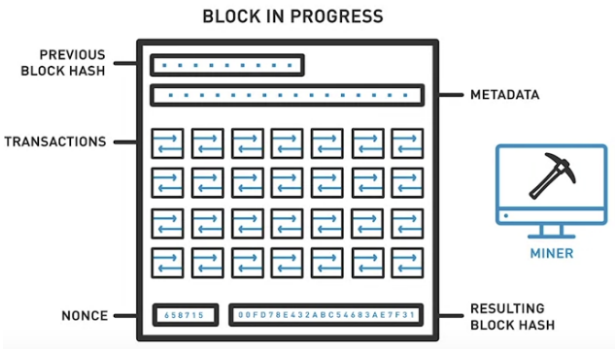
The essence of the protocol: collaboration, cryptography, and code in action.



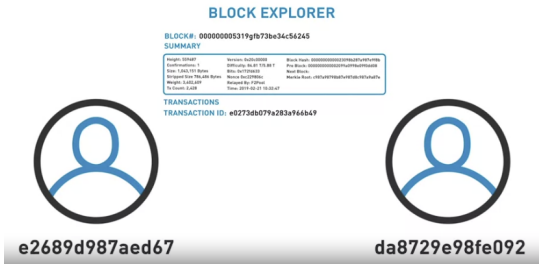




Creating a transaction message and sending it to the blockchain (2-step process: public-key cryptography)



Broadcasting the message to the blockchain network (nodes/miners - Proof of Work), verifying data (amount, sender. recipient, etc.) - Block in progress



Block completed and added/attached to the chain of blocks

Blockchain Design Principles

> But a tool like blockchain can protect much more than just money. It can document property rights. It can ensure citizenship. It can defend a person's participation in government, culture, and the economy.
>
> The first era was driven by emerging computation and communications technology. The new era will be powered by a combination of computer engineering, mathematics, cryptography, and behavioral economics.

The principles are guidelines for creating software, services, business, business models, markets, organizations, and even governments on blockchain, shaping the next era of the digital economy, an era of renewed trust.

Principle 1: Networked Integrity

On the blockchain, **trust doesn't come from an outside source. The four values of integrity (honesty, consideration, accountability, and transparency) are coded into the blockchain.** They're baked into decision rights, incentive structures and operations.

Integrity is distributed among nodes, not vested in a single member. **That means acting without integrity is either impossible or it costs far too much time, money, energy, and reputation.** Cheaters never prosper.

- e.g. needs to solve the double-spend problem
  BTC: the network timestamps that first transaction where the owner spends a particular coin. It rejects any more spends of the coin.
- e.g. needs a consensus mechanism
  BTC: Proof-of-Work.
  Miners use their resources, namely computing hardware and electricity, to solve the puzzle by finding the right hash. When someone solves it, everyone else can check the work quickly. Whoever solves the problem first gets to create the next block. And for each block a miner creates, he or she receives bitcoin as a reward.

  ETH: Proof-of-Stake.
  Proof of stake requires validators to invest in and hang on to a native token of the blockchain. They needn't spend energy to vote.

  Ripple and Stellar rely on social networks for consensus.
  They might require new nodes to generate a unique list of at least 100 nodes they can trust in voting on an update.

This type of proof is biased. Newcomers need social intelligence and reputation to participate.

There's also proof of activity, combining proof of work and proof of stake.
There's also proof of capacity requiring miners to devote a lot of hard drive space to mining.
A similar concept, proof of storage, requires miners to share their disk space in a distributed cloud.

Regardless of the consensus mechanism, the blockchain ensures integrity through clever code rather than through human beings.

Principle 2: Distributed Power

> Time and time again, central powers have proven they're willing to treat their users poorly. They override their wishes, they implement large-scale changes without consent and they warehouse and analyze their data. They also share those data with governments without users' knowledge.

The blockchain system distributes power across a peer to peer network. **There's no single point of control, no single party can shut the system down.** If over half of the network attempts to overwhelm the whole, everyone will see what's happening.

The functioning of the blockchain is **mass collaboration**. You control your data, your property, and your level of participation. **By distributing computing power, blockchain enables distributed and collective human power.**

Principle 3: Value as Incentive

The way blockchain is set up, **it aligns the incentives of all stakeholders.** It uses a token of value, like a bitcoin, to promote behavior benefiting the blockchain as a whole. **When everyone has a stake in the network, people make sure that it stays healthy.**

The blockchain breakthrough is in **using programming to incentivize good behavior.**

> Satoshi recognized that people act in their own self-interests. So, he needed to harness that self-interest to build and protect the blockchain. He programmed the source code so that no matter how selfishly people acted, their actions benefited the system. The resource requirements of the consensus mechanism, combined with bitcoins as a reward, compelled participants to do the right thing; to act with integrity.
>
> The Bitcoin blockchain also preserves value by programming its monetary policy right into the software. This means the currency is more secure. Not only is it immune to counterfeiting and theft, but it also resists inflation.

With blockchain, people have a financial incentives to collaborate effectively and to create just about anything.

Principle 4: Security

A blockchain network incorporates safety measures **with no single point of failure.** They provide not only confidentiality, but authenticity and non-repudiation to all activity. By non-repudiation, we mean the authenticity of records, like a digital signature, can't be denied.

Anyone who wants to participate in the blockchain must use cryptography. You can't opt out.
Because of how it's set up, any reckless behavior doesn't endanger everyone, it only affects the person who behaved recklessly.

If the next stage of the digital revolution involves communicating money directly between parties, then communications and transactions **need to be hack-proof**. Using **Public Key Infrastructure(PKI)** from the start makes a long Blockchain almost impossible to hack. That's the blockchain's breakthrough.

> Satoshi required participants to use public key infrastructure or PKI to establish a secure platform. PKI is an advanced form of asymmetric cryptography where users get two keys. The two keys don't perform the same function, one is for encryption and the other is for decryption.
>
> The Bitcoin blockchain runs on what's called SHA-256, a well-known and established algorithm published by the US National Institute of Standards and Technology, NIST. It's accepted as a US federal information processing standard.

Digital currency isn't stored in a file per se. It's represented by transactions indicated by a cryptographic hash. Users hold their crypto keys to their own money and transact directly with each other. Every user is responsible for keeping his own private keys private.

Other algorithms, such as proof of stake, burn much less energy, but some experts find it suspect.

> Crypto expert, Austin Hill, calls proof of stake a system where the rich get richer, where people who have tokens get to decide what the consensus is.

Proof of work on the other hand is based on physics instead of wealth, and is therefore more egalitarian. As a blockchain gets longer and longer, it also gets safer and safer. Hacking a long-chain requires substantially more computing power than attacking short chains.

Principle 5: Privacy

Privacy to us is a basic human right and it's the foundation of freedom and free societies. People ought to have the right to decide what, when, how, and how much about their identities to share with anybody else. People should control and even own their own data.

With the blockchain, the identification and verification layers are separate from the transaction layer. On the blockchain, participants can maintain some personal anonymity. They don't have to attach any other details to their identity or store those details in the central database.

Blockchain protocols allow us to choose the level of privacy that we're comfortable with in any given transaction or environment. **It helps us better manage our identities as we interact with the world. While blockchain is public, users' identities are also pseudonymous.** With every transaction, the sender can provide only the metadata that the recipient needs to know. Moreover, anyone can own multiple public- private key sets just as anyone can have multiple devices or access points to the Internet or multiple e-mail addresses. This complicates the tracing of data back to any one person or any one institution.

We could design high or low levels of transparency into any application and to any business model or set of transactions, should all the stakeholders agree that that's a good idea.

Blockchain provides a defense against the incoming surveillance society.

> Satoshi eliminated the need to know the true identities of people in order to interact with them. When Satoshi Nakamoto created the Bitcoin blockchain, he installed no identity requirements for the network layer itself. No one has to provide a name, an e-mail address, or any other personal data in

> order to download and use the Bitcoin software. The blockchain doesn't need to know who anybody actually is.

Principle 6: Rights Preserved

Rights we should and can protect. Ownership rights should be transparent, they should be enforceable. Individual freedoms need to be recognized and respected. **Smart contracts are an instrument for protecting, and enforcing those rights.**

To enforce rights, those **rights must be clear**. **Rights and responsibilities can be codified in a smart contract and placed on a blockchain.** In that way, the necessary decisions and incentives will be transparent and they'll be reached by consensus.
Now, to be sure, **this is not simply about technology, it's much bigger**. We need better education about rights and we need to understand rights management systems better.

The blockchain breakthrough is strengthening property rights by making them inarguable and unforgeable.

> On a blockchain like Bitcoin, the proof of work required to mint coins, also timestamps transactions. So, only the first spend of a coin will clear and settle. **Using public key infrastructure, the blockchain not only prevents a double spend, but also confirms ownership of every coin in circulation. That's why you can't trade what isn't yours on a blockchain.**

As a ledger of everything, **the blockchain can serve as a public registry through such tools as Proof of Existence**, as site that creates and registers cryptographic digest deeds, titles, receipts or licenses on a blockchain.
Proof of Existence doesn't maintain a copy of any original document. The hash of the document is calculated on the user's machine not on its site. That ensures confidentiality of content. Even if a central authority were to someday shut down Proof of Existence, the proof would remain on the blockchain.

Blockchain has a mechanism to handle more complex transactions involving bundles of rights or multiple parties. The mechanism is the smart contract. Smart contract is an agreement that self executes, kind of like a contract with a software, lawyer, bank and the government inside it. Think of it as a piece of special purpose code, that encodes an agreement between parties and is based on certain conditions that execute a complex set of instructions. Another way of putting this, it's a fleshing out of legal instructions executed by software. **The idea is to let software determine the legal course of action.**

Smart contracts could also handle difficult rights of shared resources among the community. Some authorized users might only be able to access and withdraw resources. Other people might have those rights but could also exclude others from access. Certain proprietors would hold management rights beyond access and exclusion. At the top would be the owners, who could access, use, exclude others, manage, and sell the resource.

Principle 7: Inclusion

The foundation for prosperity is inclusion. And blockchains can help.
Of course, inclusion has multiple dimensions.
It means participation by people of all social, economic, and racial background.
It means an end to discrimination based on health, gender, sexual identification or sexual orientation.
It means dropping barriers to access because of where a person lives, whether a person spent a night in jail or how a person voted.
It also can mean an end to glass ceilings of the old boy networks.
It means change for the better.

> Most of the world's population is still excluded, not just from access to technology but from access to the financial system and to economic activity. Despite its promise, the Internet hasn't really delivered prosperity to all.
>
> There's still 2 billion people without a bank account and in the developed world, social inequality continues to grow.

The blockchain breakthrough is making a stable payment system available to all, regardless of where they live or how much money they have.
Blockchain drastically lowers the cost of transmitting payments of any sort. They can serve as a bank account. They can help people obtain credit and invest in their future. And it supports entrepreneurship and participation in trade, even global trade.

> **Satoshi Nakamoto designed the BitCoin blockchain system to work on the Internet but it can operate without it if necessary.** Satoshi imagined the typical person would interact with the blockchain through what he called **Simplified Payment Verification mode.** This mode works on cellphones. It lets anyone with a flip phone participate in a market as a producer or a consumer. There's no bank account required, no proof of citizenship, birth certificate or even a home address, no identity. You don't even need a stable local currency to use blockchain technologies.

To keep the Blockchain inclusive **it needs to be accessible at slower data speeds.** So we must consider the full spectrum of usage not just the state of the science of high end users. But the slow tech and the sporadic power outages of users in remote regions of the world's poorest countries.

Public and Private Ledgers

A private blockchain doesn't mean full privacy, it means exclusivity of membership.
And a public blockchain doesn't mean total lack of privacy, it means all are welcome.
Transparency and privacy actually become design choices. Designers can use low tech and high tech solutions to mask transactions, whether they're in public or in private blockchains.

Introduction to Transparency

> Louis Brandeis: sunlight is said to be the best disinfectant.

In the world of blockchain, sunlight is what we call transparency. The ability to see all aspects of transactions is critical to insuring strong markets, corporations, and governments. Without transparency, corruption and scandals can grow and fester.

Transparency is the theme of Blockchain Revolution.

Transactions on a blockchain have high transparency, whether they're pubic and permissionless like Bitcoin or Ethereum, or private and prermissioned, like Ripple or Hyperledger.
This second era of the Internet, Internet of value, forces us to reconsider the benefits and challenges of public knowledge about transactions and contracts.

The Benefits of Shared Knowledge

Blockchain's most basic functions begin with **attribution, the most critical piece of both asset ownership and a contract.**
Attribution requires knowledge of two facts: who holds the asset, and who has created it and is party to the contract.
A blockchain stores this information by recording where the asset originated and tracking changes of ownership.

- Ownership is attributed to an address or public key. An address is like an identifier. It's made up of a simple set of letters and numbers. In principle, the addresses and identities are what's called pseudo anonymous.
- Transactions recorded on blockchain means multiple parties within the network can see past actions and current ownership of assets.

This distributed ledger, as opposed to a centralized database, creates a network of shared knowledge. Everyone in the network can see it building in transparency.

Disclosure is a natural process and added benefit of blockchain-based transactions.

> Audits are time consuming, and they're expensive.

On the blockchain, all transactions are recorded and stored in an immutable trusted ledger. If we reduce information asymmetry and increase shared knowledge, we can use resources more effectively elsewhere.
Blockchain technology can therefore be a catalyst for the greatest benefit of all: growth.

How Much is too Much Transparency

By enhancing transparency in transactions, blockchain creates both challenges and opportunities.
Shared knowledge enhances attribution when it comes to assets and contracts. Reducing information asymmetry can cut company risks and costs, and spur economic growth. But for all of the transparency's virtues on the blockchain, it also has its downsides.

e.g. Financial markets depend on some level of anonymity. In certain markets and with certain use cases, some level of privacy is required. Transparency has the power to affect economic interactions between market participants.

The alternative to a public blockchain is a permissioned, private blockchain. It's organized and controlled by a known and trusted consortium of entities. The assumption here is that the level of visibility is a design choice, but it's not that simple. A private blockchain still involves the record keeping of everyone's transactions by each node of this network.

Anyone with privacy concerns faces the same challenges using the Internet every day, and the Internet is widely used.
Instead, our discussion around transparency should f**ocus on the desired socially optimal level of transparency.**

Choosing this proper level is critical for firms wanting to launch a private blockchain. Though, changes in transparency have economic consequences. They create winners and losers. That's why regulators and lawmakers need to think carefully about what disclosure they want to require of corporate users of blockchains.

Native Transparency in Blockchain Technology

Centralized Registries vs. Distributed Ledgers

Centralized ledgers require third parties because they lack transparency.
Distributed ledgers are transparent by design, and therefore promote consensus amongst all parties.

Recording transactions and ensuring consensus on the current owner of an asset, is one of the key features of blockchain. It's an **append-only protocol**, **allowing no changes to existing records**. This setup defines who can enter records on the ledger and under what circumstances. It then stores these transactions

Public vs. Private Ledgers

Centralized Data Storage

Most firms still store enterprise data in a centralized database. It's a simple setup having one location. Every time a transaction occurs, it must clear and settle through this intermediary. This prevents one party from selling the same asset or spending the same dollar twice. For all its simplicity, concerns with central database remain the same with security at the forefront. **Anything that is centralized is vulnerable to hacking, attack or fraud.** The upshot is, data goes missing or personal information gets stolen. **So, keepers of central database is always make backups.** A backup model is one step closer to a distributed database in this one

sense. Keepers need to update backups continuously to avoid losing data. **So we need some sort of backup protocol to ensure the data's accuracy.**

Distributed Database

In a distributed database, there's **no single primary location** where all changes can originate. Instead, each site can make changes to the data but all stakeholders must agree through consensus. There are several advantages to this setting.

1. there's no single point of failure.
2. all data are available locally
3. the system can be set up so that the different locations need not trust one another, even as they agree on the content of the database.

A major side effect of distributed ledgers is that others in the network can see some of your information. To ease this fear, **we need to understand what the information reveals.**

Storing information is not equal to accessing it. We can choose from two types of distributed ledgers, the **public ledger and the private ledger.**

Public Ledger

A public ledger is permissionless. Permissionless means that anyone can become a network node or participant and anyone can in principle enter records in the ledger. That makes them inclusive.

The bitcoin and Ethereum blockchains are the best-known public ledgers. Becoming a network node is just part of using blockchain.

Public blockchains record all transactions with the addresses of buyers and sellers. This information is kept at each node and shared across this wide network. This transparency prevents data loss and encourages consensus among parties. **Public blockchains are open innovation. Anyone can push a change to the code base and if the network participants agree, that change can be integrated.**

Private Ledger

A private distributed ledger, on the flip side, is built by either an individual enterprise or by a consortium of organizations. It differs from public distributed ledgers in several key ways.

A private network requires permission. Thus it restricts who can use it to record transactions and who can see the flow of information and assets.

For financial institutions, this is an important feature. It allows them to comply with know-your-customer rules along with Anti-Money Laundering rules. These networks also don't need a trust-less protocol. **This is a downside in one way because a consortium solution raises the threat of collusion as well as rent extraction typical of a trust.**

But **we can't assume that private distributed ledger guarantees privacy**, it can't. A private blockchain has some of the same features as a public one. **The network can still see information and transaction records. It's just a matter of deciding who should be included as a member.**

Transparency as a Risk and an Asset

Transparency as a Strategic Risk

Transparency increases the risk of firms imitating each other's trading strategies. Blockchain's transparency may be viewed as a hefty risk in the financial world, but it can be really useful in other areas.

Transparency as a Strategic Asset

What does transparency mean in the business world?

> Denise Parris, a professor of entrepreneurship, defines transparency as, the extent to which a stakeholder perceives an organization is providing learning opportunities about itself.

With blockchain technology, firms benefit from transparency both directly and indirectly.

Indirect benefits help **foster relationships growing in value over time**. Establishing and publishing a code of ethics is a great first step to achieving this. It will inform employees and customers of what to expect from business dealings.

There are five specific elements for a firm to achieve success through transparency.

1. creating true value that withstands scrutiny
2. understanding customers and building relationship capital
3. protecting consumer privacy
4. acting with integrity
5. being candid about shortcomings

Sharing relevant information with partners and supply chain members quickly improves trust and can generally lift a firm's brand and reputation.

These principles apply in a world where financial transactions and contracts are visible on a blockchain.

Recording transactions and holdings on a blockchain also has lots of direct procedural advantages in market interactions. Greater transparency in this market could increase liquidity, could improve price discovery and ultimately reduce origination costs for new issuers which would be a boon towards entrepreneurship. But of course this is not just for finance.

Blockchain enables a market-based solution when all financial obligations are visible.

Approaches to Privacy in Blockchains

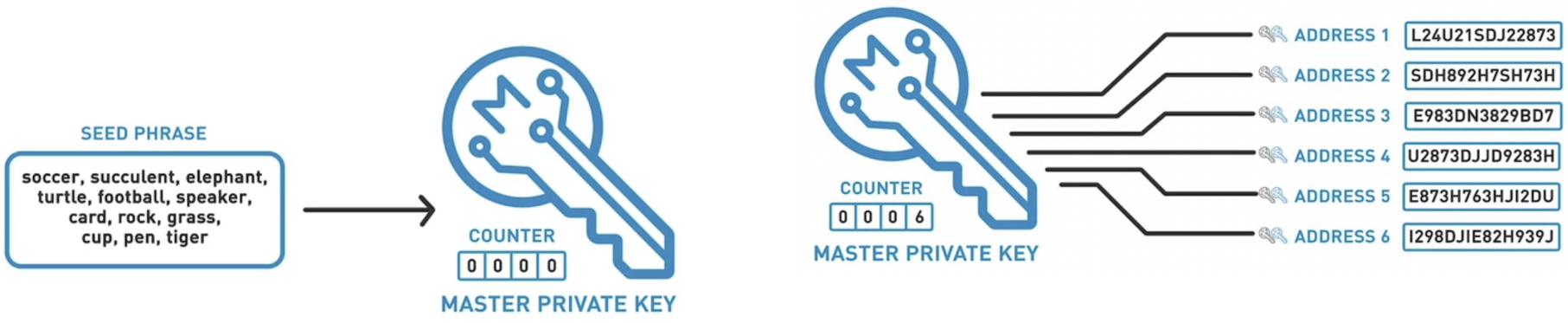
Usage of Multiple IDs (Low-tech Privacy Solutions)

Distributed ledgers are not necessarily set up to guarantee privacy for users. Transactions can be traced by looking at the different addresses in that transaction.

Are actions on blockchains always fully traceable with full attribution? The answer is, of course, no.

There are some simple workarounds that can improve privacy and transactions.

Hierarchical Deterministic wallets or so-called HD wallets.
Hierarchical deterministic wallets have also been proposed as a solution to privacy in private distributed ledgers. **An HD wallet uses algorithms to create a new public-private key pair for each transaction or piece of a larger trade. This thus would allow a user to have a virtually infinite number of public addresses all derived from a single master seed phrase, making their identity difficult to trace.**



Another HD wallet solution to generate privacy is a so-called **merge and re-split operation**.
In this example, several entities anonymously submit new addresses to a smart contract. The contract collects the same amount from each party. Then the contract re-deploys the amount to the new addresses. From the outside, we wouldn't be able to follow the

trail of money beyond that point. Now, this is useful for many financial services and enterprise use cases, but in a completely uncontrolled and unregulated public environment could potentially run afoul of the law.

How do you create a system where digital assets can be moved peer-to-peer, but still with some complete measure of privacy, all in a regulated way? Well, consider using **a permissioned blockchain**. On a permissioned blockchain, IDs would be known, and a regulator or some authority could have insight. But you could shield your behavior from unwanted outside observers, such as your competitors.

Zero Knowledge Proofs(High-tech Privacy Solutions)

A zero-knowledge proof is a sophisticated method for authenticating a transaction without revealing much details about it.

Pioneered by Zcash, zero-knowledge proofs are catching on in other platforms. For example, developers of the public blockchain Ethereum are already including the option to use a generalized version of zero-knowledge proofs on their own blockchain.

The concept they employ is something called **zero-knowledge succinct non-interactive argument of knowledge**, or, conveniently, **ZK-SNARK.**

A ZK-SNARK is a zero-knowledge proof protocol. It lets users reveal only the necessary information to the verifier and no more.

Linkable Ring Signature(High-tech Privacy Solutions)

Another high-tech concept offering privacy is a **linkable ring signature**.

A ring signature is created when the sender of a transaction is mixed together with a random collection of other IDs that basically serve as a decoy. **This process produces a unique digital signature for the transaction, but it blurs the identity of the real sender. In signing the transaction, the sender can prove that she's the rightful owner of the assets being sent without revealing which ID is hers.**
Linkability also prevents double spending.
Monero is an example of a blockchain-based cryptocurrency offering this alternative.

Implementation in Public vs. Private Blockchains

> Privacy is a right for private citizens in many democracies. Yet, lots of jurisdictions, like in Canada and the United States, limit the privacy of corporations and corporate executives.

The procedural solutions for privacy like using multiple IDs are central to public blockchains, the downside of multiple addresses is that privacy comes at a high cost. Identity creation may be free but the transactions come with fees.

The struggle to be transparent, yet protect our identities and our trade secrets continues to be one of the greatest challenges of implementing blockchain, whether it's a public or a private one.

There's procedural workaround from public blockchains can apply to private or permissioned blockchains as well, but private blockchains provide further options.
Whether a user can create multiple IDs is really just a design choice. The economic incentives for proof and settlement of transactions is also a design choice, that includes the cost for using multiple IDs. Private blockchains may have features for masking user identity or features limiting visibility of transactions only to certain parties. More critical for private blockchain is this, users must understand the identity setup. They must understand the network governance and the information available to all network members.

There are two main outcomes to consider as blockchain technology and the financial industry evolve.

1. private, permissioned blockchain networks in which verified, non-anonymous nodes can post transactions to the ledger and confirm other transactions.
   Such networks are typically also read limited to that same network of verified nodes, but the network could allow a larger audience to read the data. A subset of that network could allow further control over read and write access, so that I can use a much simpler form of consensus, one based loosely on a supermajority vote of the nodes rather than on the more CPU intensive proof-of-work system.
   Such a network can also accommodate a much higher transaction volume than that which is typically provided by proof-of-work blockchains.
   Many of those building distributed ledger applications for the financial industry and for the Industrial Internet of Things prefer this model.
   It may also prove more valuable for those building certain public facing applications.
2. financial institutions and other enterprises could design a distributed ledger similar to their current system, essentially moving what they've got to a new technology platform.

Private blockchains hold lots of promise and will likely be widely used. **However, they have some disadvantages that must be acknowledged, for one, they can become large, lucrative targets for hackers.** Now, depending on the protocol a single compromised member could expose the whole network, though distributing consensus across many members should make this more difficult.

The Blockchain Ecosystem

> Internet:
> **Governance, meaning, stewardship, collaboration, and incentives to act in our common interests.** Without governance, the internet wouldn't be what it is today, a global network of interoperable networks all using the same standards and protocols. **No government controls the internet, it's managed by an ecosystem.**

Governance of blockchain on three levels.

Blockchain stake holders can apply Internet's Governance Model today and in doing so, they can overcome many of the showstopper and safeguard this technology's future.

> In 1992, computer scientists David Clark said, "We reject kings, presidents, and voting. We believe in rough consensus and running code."
> This philosophy for governing the Internet as a global resource, was a huge shift away from the usual way of doing things.

Centralized paradigms, aren't as effective in the digital age. The creation of an open-source Internet was a bellwether. It was a dramatic departure from the traditional hierarchical structure. It was decentralized and yet it worked.
The second-gen Internet, is just as enthusiastic about **openness** and just as disdainful of hierarchy. Satoshi Nakamoto, Erik Voorhees, Nick Szabo and other pioneers embraced much of the same **self-sovereignty** that Clark espoused decades ago.

As with the Internet, the blockchain ecosystem contains lots of competing viewpoints. Even the core blockchain contingents, have kind of split. Different crypto camps are advocating their own agendas and the fine details are lost in translation to a novice public at large.

A great organizing principle, is not on its own an agent of progress. Open-source governance has transformed society and we will need coordination, organization, and leadership.

Code alone is just a tool. It is humans who must lead. We need all stakeholders in the blockchain ecosystem to come together.
We have serious unanswered questions. We need to address mission critical issues.
How will the technology scale?
Can we scale it without consuming too much energy?
Can we agree on standards without reverting to hierarchy?

Governance networks are the answer not state-based institutions. Diverse stakeholders can effectively steward a global resource with inclusivity, consensus, and transparency. Block chain stake holders in civil society, the private sector, and governments can and should collaborate. Call these collaboration's Global Solution Networks(GSNs). Such networks can achieve new forms of cooperation, social change, and even produce public value.

Blockchain Stakeholders

Mathematics is no longer blockchain's sole regulator. **A broader focus on governance is a good thing, even for crypto.**

1. Industry Pioneers
2. Venture Capitalists
   The success of insiders caught the attention of Silicon Valley's brightest venture capitalists.
   They include the venerable Andreessen Horowitz and many others.
3. Banks and Financial Services
   Now financial services titans have joined the mix. Goldman Sachs, the New York Stock Exchange, Fidelity, Visa, Barclays. The United Bank of Switzerland, CIBC, TMX Group and dozens of others have invested in startups, launched projects, or joined consortiums. Pension funds have likewise entered the fray.

   A more dramatic reversal of opinion happens in banking. For the longest time many financial institutions just dismissed BitCoin outright. They considered it the currency of gamblers and criminals. Blockchain wasn't even a blip on their radars. Today, really, they're all in on blockchain and many are even coming around to BitCoin and other cryptocurrencies. It was really quite incredible to watch this unfold in real time. Few major financial institutions saw fit to invest before 2015. Now dozens of global institutions have invested in this technology. And they've also come to participate in leadership discussions. Many of the world's biggest banks join the R3 Consortium.
4. Developers
   Former Bitcoin core developer Gavin Andresen became a reluctant public advocate during the so-called hash wars of 2016 and 2017. The work involved a lot of outreach and lobbying. Andresen admitted Internet governance is kind of chaotic and messy but it work, and it's reliable.

   Micropayments, stock trading, property transfer, and many other businesses depend on addressing and overcoming technical standard issues within bitcoin and the broader blockchain world.
5. Academia
   Academic institutions are funding blockchain studies in labs and centers. They're diversifying by collaborating with colleagues outside their silos.

   Joichi Ito, Director of the MIT Media Lab, saw the opportunity for academia to play a role in things. He said MIT and the academic layer can be a place where we can do assessments, do research. And be able to talk about things like scalability without any bias or any special interest.
6. Leadership
   Leaders like Arianna Simpson, former head of business development at BitGo, who is now an investor in the sector. Kathryn Haun is a General Partner at Andreessen Horowitz. Many of these leaders have suggested that the industry welcome all voices. **It's of the utmost importance that the trend towards diversity and inclusion continues.**

   Elizabeth Stark is arguably one of the industry's most influential players, having co-founded lightning Labs, which is developing the Lightning Network. Perhaps the single most important innovation that will scale the power and potential of Bitcoin, and as a

result all blockchain platforms. Stark has organized scaling Bitcoin to convene stakeholders in this industry. Scaling Bitcoin was credited with clearing log jams in the block size debate. It was considered a constitutional moment for the sector.
She's expressed concerns over governance. She said newcomers are simply able to do things regulated institutions cannot. So we need to think very carefully about why those regulations exist, what purpose do they serve, before we think exposing consumers to unregulated financial activities is a good thing. Ultimately, the debate is not about the kind of society we want. **It's about the present opportunities leaders have before them to steward an important global resource.**

7. Users
   Security, privacy, identity, human rights and the long-term viability of this technology. Fair hearings and fair judgments. Righting wrongs and for fighting criminals.

   We first need to coordinate and agree on the basics. Everyone seems divided on some basic taxonomy.

8. Governments and Regulators
   Now, the world are uncoordinated. Some are laissez faire, others dive right in with rules and regulations, like the BitLicense in New York, with unintended consequences that can stifle innovation. Some regimes are openly hostile. China has banned cryptocurrency exchanges outright, even though cryptocurrency mining is still widespread in China and blockchain innovation is frankly exploited.

   Likewise, the industry is split. There are those who support new rules and those who don't, and they fall into various factions. Even those who resist government intervention do concede any government enthusiasm can be a positive. Prolific venture capitalists, Adam Draper, said, "Government endorsements create institutional endorsements that has value."

   Central Banks, despite their different approaches to blockchain, are more welcoming of governance.

9. NGOs and civil society organization
   Focused specifically on transformation through blockchain technology.

When we talk about **governing** blockchain technology, we're **not only talking about regulation**. Regulations alone can't control an important global resource, nor should them.

> Joichi Ito said, "You can regulate networks, you can regulate operations, but you can't regulate software."

So, regulations will be just one of several important pieces in the blockchain governance puzzle, a puzzle that is yet to be fully assembled.
We've seen lots of parallels in origin and ideals between the Internet and blockchain technology. But blockchain is not entirely like the Internet because money is different from information.

Stewarding the Blockchain Revolution

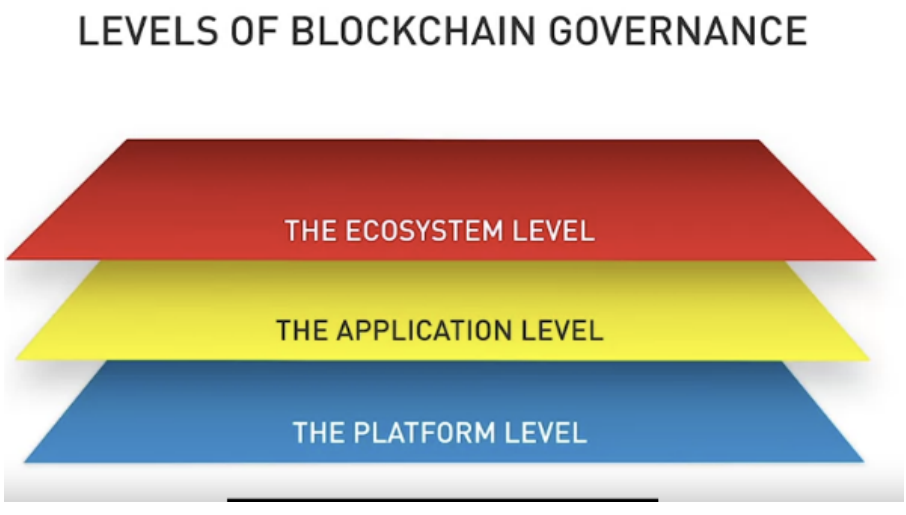
We think the future is not something to predict, it's something to achieve, we all need to get involved.

The early days of blockchain were unregulated like the Internet of days past, where innovation soared and a whole ecosystem grew. Yes, eventually, regulation found the Internet. Those regulations are important and can be beneficial to society.

Now blockchain's ecosystem has matured a bit. It's time to make sure this technology last.
Blockchain's next era may require even more government involvement than did the Internet. There's a reason for that.
The Internet of information deals with just that, data.
Blockchain, as the Internet of value, deals in assets, money, identity, land, diamonds, things of value that are critical to the economy.

The Internet of value requires stewardship and not just the one but three distinct levels. These are the platform level, the application level, and the ecosystem level.

The platform level calls for self-governance. Platforms should develop standards, use cases, and robust roll-out. We have seen vital movement on this level in recent years, the bitcoin community fort and applies different solutions for

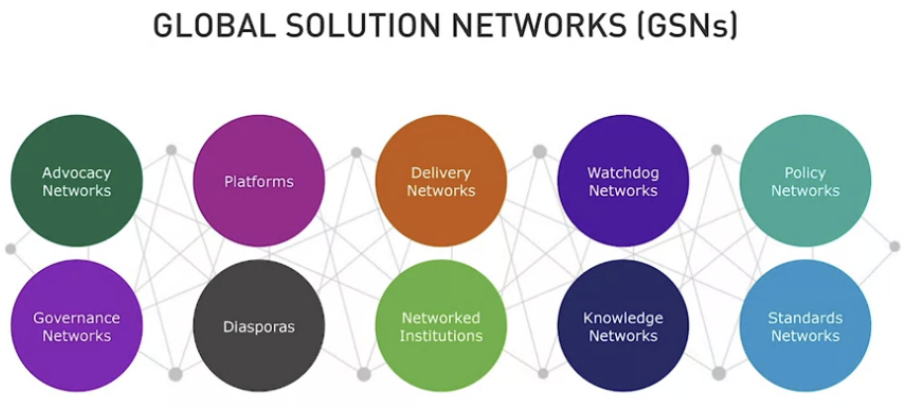


scalability. The Lightning Network sees rapid expansion and development. Ethereum has already tested its crisis management by consensus and plans a proof-of-stake roll-out, and Hyperledger calls for urgency around standards with a measured approach.

At the application level, various blockchain consortium have come together.
Brands like FedEx or Pepsi have joined with industry partners and even their competitors to develop standards and common applications.
The enterprise Ethereum Alliance works to build application level standards for platforms using Ethereum.

The overall ecosystem level as networks like the Blockchain Research Institute creating and circulating knowledge. This level is also home to advocacy groups like the Global Blockchain Business Council or the Chamber of Digital Commerce.

Blockchain needs to be self-governed primarily using a multi-stakeholder approach - Global Solution Network(GSNs).



First, use standard networks to codify your common ground.

Second, use network institutions' complex organizations that do many things to welcome stakeholders with radically diverse views on what needs to be done.

Third, use advocacy networks to respect each other's interests and constraints, and to advocate for the right thing to do.

Fourth, watchdog networks can be used to make sure no one does any harm.

Fifth, use policy networks to join policy debates and coordinate regulation.

Six, use knowledge networks, networks that create and extend knowledge to get up to speed.

Last, use what we call delivery networks to keep incentives for mass collaboration in mind.

Blockchain Implementation Challenges

Overcoming Showstoppers

Showstoppers are obstacles to development and widespread adoption of blockchain technology.
Showstopper are also risks to the decentralized control and openness of blockchain.

If we look back at the history of disruptive technology, we see many examples of innovations gone bad. Their inventors were attempting to solve a problem plaguing humankind. But innovations like big ideas can be twisted or applied in ways their inventors never intended. New technology can be used for good and for evil.

Challenge 1: The Technology is Not Ready for Prime Time

Some people still have a vague understanding of cryptocurrency. Even fewer have heard of blockchain technology.

8 key issues:

1. The technology of the future is already here but its infrastructure is unevenly distributed.
2. The system lacks the transactional capacity for mass usage.
   The blockchain would also be prone to capacity problems, systems failures, unexpected bugs and the frustration of non tech savvy users. Some platforms like Ripple and Hyperledger have gone a long way in solving these problems. And up-and-comers like Cosmos may change the game. But this is a still a concern for some applications.
3. Inaccessibility to the average person
   There's not enough wallet support and a lot of interfaces aren't yet user-friendly. They're in complex code and tech jargon. Bitcoin addresses may ultimately need to have a similar simplicity of use.
4. Lack of liquidity
   For example, there will be 21 million Bitcoins in circulation by the year 2140. But it will be mined at a decreasing rate. As the number of users grows, the value per coin is likely to grow. Early adopters hold on to bit coin as miners hold onto gold. They hoard it, hoping the value will increase, rather than treating it as something to exchange. There is also the dilemma of coins stores in lost wallets or sent to addresses whose owners have lost their private keys. These coins can't be recovered. And that means there will be fewer Bitcoins in actual circulation than the 21 million.
5. High latency
   It takes on average 10 minutes to clear and settle transactions on the Bitcoin blockchain network. It's faster end-to-end than most other payment forms, but it's still too long for certain use cases like the Internet of Things. Where devices need to interact non-stop. Ten minutes is just too long to retail financial transactions where timing matters to get an asset at a particular price.
6. The behavioral change required well beyond net etiquette
   Bitcoin provides better privacy, stronger security and more freedom from third party cost structures and systems failures. But with greater freedom, comes greater responsibility. Unlike Bitcoin users, average people aren't used to backing up their money on an hardware wallet. In so-called cold storage, disconnected from the internet.
7. Societal change
   Money is a social construct, representing what a society values. It's a vital part of our social structure because it's molded by our relationships, and it adapts to our evolving needs. So is it really socially unhealthy to create an immutable record of every human transaction in perpetuity? Remember, the blockchain never forgets, it appends, but it never erases.
8. The possible lack of legal choices in a world of transaction finality and unstoppable smart contracts.
   Smart contracts can insure a transaction goes through with mathematical certainty, but it allows no room for human doubt or regret. This unprecedented approach means that blockchain users can decide which rules to follow. But once they decide, once they execute a smart contract there’s no backing out.

Challenge 2: The Energy Consumed is Unsustainable

The proof of work consensus mechanism used by the Bitcoin Blockchain ensures network security. These protocols are not only the unique building blocks, they are critical building blocks of people's trust in the system.

The energy used to show proof of work is significant, **and if it scales linearly, it will be unsustainable.**

Hashing, the process of digesting transactions through the secure hash algorithm, known as SHA-256, and solving a block, burns a lot of electricity. Critics suggests that we could be using it to cure cancer or explore the stars, instead, we're using it to process Bitcoin transactions.

We need to find the best way to solve for the electricity needed to run and cool the computers mining Bitcoin and securing the Bitcoin network. Hash rate is only one way to measure the processing power of the Bitcoin network. The hash rate has risen significantly since Bitcoin's inception. As it increases, the trend is towards using more energy, not less. When we get down to it, all forms of money have a relationship to energy. We just have to decide if the blockchain is worth the costs.

The second energy-related issue is computer architecture. The Bitfury Group has built a Bitcoin solver with application specific integrated circuits, or ASICs. These are energy efficient designed solely to mine Bitcoin. Another environmentally friendly factor is the location of the mining equipment. Relocating to cooler climates may help. Although these initiatives may limit mining carbon footprint, miners who want to make a career of it must continually to upgrade their systems. Most mining equipment remains competitive for less than a year.

If Bitcoin truly becomes a global network for payments, some developers believe they'll need to move away from proof of work as a security measure and find an alternative mechanism. The purpose of consensus algorithms is to allocate the right to decide the state of the blockchain network to a decentralized set of users.

> Vitalik Buterin, co-creator of Ethereum, **sees only three securely decentralized sets of users. Each set corresponds to a type of consensus algorithm.**
> The first set is owners of computing power with standard **proof of work** algorithm.
> The second set is stakeholders with various **proof of stake** algorithms.
> The third set is members of a social network with a **federated style consensus** algorithm.
> These systems don't burn electricity as the blockchain does for Bitcoin.
>
> The fourth way to address energy waste is **proof of disk**, where owners of disk storage space define the economic set of users.

The choice of consensus algorithm must achieve two goals.
One, it must keep the network secure
Two, it must distribute the decision on network status widely to the most appropriate decentralized economic set.

Challenge 3: Governments Will Stifle or Twist It

In the past, governments have successfully stifled centrally controlled networks.

Law makers attempting to introduce laws or policy without fully understanding the technology is a recipe for disaster. By not understanding blockchain's potential, new legislation can actually harm its development.
The courts have already got it wrong, they've tried applying intellectually property rules to Bitcoin, but it has no intellectual property elements. There's no creative spark for copyright. There's no patentable idea. There's no patent and there's certainly no trademark. It was born of the public domain and released to the public domain.

> Bitcoin creator, Satoshi Nakamoto, viewed this blockchain experiment as a new path toward freedom, not total upheaval. Cryptography is not a solution to the world's political problems, he said.

The learning curve for governments is steep, but it is less though for dictators looking to create machine driven despotism.
On the one hand, lawmakers must not stifle innovation for fear of the possible abuses. Human trafficking, illicit drug trade, gun running, child pornography, tax evasion, money laundering, counterfeiting and the coordination of terrorists or white supremacists. These are all worst case scenarios, and they're looking to exploit all innovations, not just blockchain.
On the other hand, government must not twist untested applications, like blockchain base platforms for identity management, to infringe on or restrict civil liberties. They already appear to be doing this in China with a social scoring system.

Jurisdiction is already an issue with Bitcoin. How should cryptocurrencies and other digital assets and their sale and transactions be regulated? Most government leaders and regulators do not understand the power of this technology innovation, and for economic and social development.

Bitcoin isn't illegal, but it could be at any moment.

We need a stable approach to regulation, legislation, and international negotiation. We need investors to remain confident and continue to support the technology's global development.

Legal frameworks also matter. Legal scholars don't think that the current framework can handle certain questions raised by smart property on a global scale. Smart contracts both define and manage ownership rights. Their code makes no assumption about the transfer of those rights. Code can't randomly seize, divest or transfer these rights.

Another concern is identity in the blockchain. Identity matters big time, but people mostly have a simple view of identity. If governments transfer identity to the blockchain, where information is fixed, we actually end up with a technological construct not at all like the social construct of identity. It'll become a terrible tool for fashions. Combining a precisely coded version of personhood with a precisely coded version of society is the stuff of the science fiction novels. Self-enforcing contracts, walled gardens or trusted systems owned and managed by privileged, decentralized groups could dictate what people could or couldn't do. Constitutional safeguards or constraints would be non-existent. We'd no longer be free, more like slaves to a tyrannical regime.

Then there's the dictator's learning curve

It's not what we do with the code, it's what we don't realize we're doing with it, the unintended consequences.

Challenge 4: Powerful Incumbents of the Old Paradigm Will Usurp It

Blockchain technology has emerged as an important global resource, but it's also a disruptor. Any tool of consensus like blockchain will be vulnerable to powerful interests.

There have been a lot of concerns about the first generation of the internet, one of the biggest fears is that powerful corporations will capture most of the technology and use it to fortify their private empires.

Big companies promote and prosper from consumer transparency, but are secretive about their own activities and data assets. Yes, some companies have disclosed information about their operations, but the majorities want either to remain in the shadows or react when whistleblowers and investigative journalism shine a light on their dubious practices. The blockchain could very well become the next tool these corporations use to mark their territories.

> John Acton, "Power tends to corrupt, and absolute power corrupts absolutely."

We must all work to be good and fair stewards of change and uphold the freedom of the blockchain against any powerful and corrupt incumbent.

Challenge 5: The Incentives are Inadequate

The incentives are inadequate for mass collaboration.

Every node in the network can validate transaction. What miners do is preserve the distribution of power. This is the power to decide which transactions to include in each block, the power to mint coins, and the power to vote on the truth.

The network gets good value for miners in exchange for large sums of Bitcoin. This has actually become quite a big business. Initially, mining something like Bitcoin only required some spare CPU processing power. Now, large companies spend millions of dollars building specialized chips to compete in a huge global market. But is the incentive going to last? If it goes away, how will the network stay so secure?

The mining cycle depends on the market price of Bitcoin. When the price drops, some Bitcoin miners park their supply. Adjustments to the difficulty level mean that mining will probably always be profitable for some, but certainly not for all miners. Some miners can't afford to just park and play, they just dry dock their mining rigs or divert their processing power to a more profitable use case, sometimes mining another coin. Some join mining pools to combine their computing power with other nodes in the hopes of increasing their odds of solving a block. It's better to get a fraction of the winnings than no winnings at all.

How do we stop miners from abandoning their work? One answer is to charge fees.
The total number of Bitcoins that will ever exist is predetermined. So, once all Bitcoins have been minted, fees will likely become common for on-change transactions. Indeed, fees are already common for some transactions today. Transaction fees will support miners, but will pass through to users. **Transaction fees reflect the marginal cost of verifying a transaction. If the block rewards keep halving and there's no incentive for miners to continue, then the hash rate would likely drop. If hash rate drops, network security declines. Without network security, trust in the block chain will be lost.**

Coin exchanges are typically the biggest stake holders. **Attacks on proof of stake models come from concentrated coin control,** and this is why in some jurisdictions, exchanges must be licensed and watched by regulators.

Challenge 6: Blockchain is a Job Killer

The blockchain could become an amazing platform for radical automation. Computer code rather than human beings could do the work of managing assets and coordinating talent. The overall consensus is that innovation will create the next generation of jobs in the long run.

> PWC expects robots and artificial intelligence to replace up to 38 percent of US jobs over the next 15 years.

Blockchain platform has the potential to abolish tens of thousands of jobs of professional services firms in auditing, accounting, and finance. New business and employment opportunities will arise from the shift through the creative destruction of the market, but this is certainly not guaranteed. The key concern remains, will blockchain lead to job loss, especially in the short-to-medium term, as many traditional roles inside of these intermediaries, become obsolete? Not if we begin preparing now for the opportunities ahead.

Overall, what matters is not whether new capabilities exists, what matters is the extent to which we turn these capabilities into social benefit. Maybe we need a new social contract, redefining human work and how much time we should all spend making a living. Is it really 40, 60, or 80 hours a week?

Challenge 7: Governing the Protocols

Unlike the internet, **the Bitcoin community doesn't have formal oversight bodies who helped guide its development, and some in the community actually prefer it that way.** Most innovators and supporters can agree, blockchains openness security and decentralization are its greatest strengths. What they can't seem to agree on is how this evolving technologies should be governed, if at all. **A lack of governance adds to the uncertainty.**

Governance involves setting standards, advocating and adopting sensible policies, developing knowledge about the technology's potential, watching out for bad actors and actually building out the global infrastructure.

If the Bitcoin blockchain is to scale and remains secure. Trying to bootstrap or change a network protocol is a mighty task. Too quick or too large change on the system is a costly risk. Like the Internet, the blockchain will most likely have a messy chaotic governance process.

> A dedicated team led by Elizabeth Stark was developing the Lightning Network, a second layer protocol built on top of Bitcoin. **The Lightning Network allows participants to build payment channels, peer to peer, batching transactions, and then confirming them on the Bitcoin main chain. In other words, potentially solving the scaling issue.**

Challenge 8: Distributed Autonomous Agents

There is possibility of distributed autonomous agents going rogue. These are entities that use intelligent software to manage and organize resources and processes. Many of these highly distributed enterprises deal with a range of good and bad actors.
As the blockchain evolves, bad actors have emerged. They threaten network security and public safety. Their existence raises questions about the liability of these distributed enterprise models.

Let's explore a scenario, where we own a decentralized web hosting company. Each of the servers has a say in company management. When a human hacker or piece of malware pretends to be a million servers, it could outvote real servers in the network. This malicious entity would now control our company. It could cash out. It could attach names to otherwise anonymous data. It can hold operations for ransom until we human owners paid up.

How does society govern and control these entities to prevent hostile takeovers or deadly scenarios?
We don't think the answer is broad regulation of distributed autonomous entities or the Internet of Things. **We believe the answer lies in app developers detecting any major public impact in source code and designs.** We think they should consult with customers to anticipate and minimize risks, identify alternative paths forward, and build support.

Challenge 9: Privacy

The blockchain has great potential for ensuring anonymity and providing a degree of openness.
But we've seen corporations act like Big Brother, spying on us and calling it customer intimacy and big data analytics.
Governments are also tracking our movements through our mobile devices and tapping our data through our telecom and internet service providers. Why should we expect them to respect our privacy on the blockchain?

> Fool me in the first era of the internet, shame on you. Fool me in the second era of the internet, shame on me.

In the blockchain world, we could have better control over our data.
But do we care enough about our privacy? Are we willing to take responsibility for managing it?
The truth is none of these privacy challenges are showstoppers if we focus on design.
We can design an Internet without further eroding our civil liberties.
It can be free, in the best sense of the word, if privacy is made a default setting.
Privacy does not need to be a casualty of national security.
We can make sure every IT system, every business practice, and all infrastructure protect individual privacy by design.
It's time for leaders to **prevent rather than reacts to violations of our privacy.**
It's time to **design transparency into all corporate and government operations.**
It's time to flip the model; **black boxes for individual data managed by individuals, glass houses for organizational data, viewable by all stakeholders.**
This will take effort and advocacy.
It means scrapping permanent mass surveillance as a business model.
It means pushing laws through a rigid legal system.
It means mass activism to enact change.
We must focus on designing privacy into the stack. We need privacy protocols, not privacy patches.

Challenge 10: Criminals Will Use It

The blockchain is decentralized, relatively fast and peer to peer. A seemingly good fit for criminal exploitation.

> Silk Road, a dark web market place for illegal drugs. At its peak in October 2013, Silk Road had nearly 14,000 listings priced in bitcoin. Products were delivered by mail. The site provided a guide of how to avoid getting caught by authorities. When the FBI seized the site, the price of bitcoin plummeted.

Digital currencies became linked with crime, even though today only a tiny fraction of crimes take place in cryptocurrencies. And the vast majority of cryptocurrencies are used for entirely legitimate purposes. It is really a branding challenge that needs to be overcome. In fact, digital currencies could actually help law enforcement.

Digital times do lead to digital crimes. If human beings want to exploit other human beings, they will use the latest means to do it, if their old ways no longer work. Regardless of blockchain's critics, keep this in mind, the leading form of payment among criminals is still just cold hard cash.

Bitcoin and blockchain technology could actually discourage criminal use in a major way because of transparency and traceability.

Technology doesn't really have agency. It doesn't want for anything. It doesn't choose sides.

> When someone robs a bank, we don't blame the money sitting in the vault.
> We can't close banks just because there's a possibility they may be robbed.
> Life goes on. **We accept the benefits alongside the risks.**

That criminals use bitcoin speaks more to the **lack of strong governance, regulation, advocacy, education, and legitimate economic opportunity than it does to bitcoin's underlying virtues.**
Money is a technology after all.
We should fix the social and economic problems at hand, not ban the technology.
Indeed, bitcoin and blockchain could help us address these problems and potentially much more.

Reasons?

The obstacles facing the blockchain are formidable. Let's consider quantum computing. It combines quantum mechanics and theoretical computations to solve problems. It can factor very large numbers rapidly and efficiently. It's vastly faster than today's computers. It'll be able to crack the codes securing such assets as blockchain wallets and nuclear missiles. There is a race to make blockchains quantum resistant if not quantum proof before quantum computers become widely available.

Technology does not favor inequality or structural employment. While technology can change business and society dramatically, it doesn't determine outcomes one way or the other. **That is a function of social, political, and cultural forces.**
Throughout history, **the arc of technology has been broadly very positive.** We've made lots of advances in food and medicine. Technology has made for greater human equity, productive capability, and social progress.

> Steve Jobs. "Technology is nothing. What's important is you have a faith in people, that they're basically good and smart. If you give them tools, they'll do wonderful things with them."

Despite all these implementation challenges, the blockchain is capable of wonderful things.
