2. Blockchain, Cryptoassets, and Decentralized Finance

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

Cryptoassets

A cryptoasset is a digital asset created, managed, and traded on a blockchain. Furthermore, cryptoassets are just one facet of the financial services revolution.
Asset classes with notional values of trillions of dollars, stocks, bonds, collectibles, and currencies, just to name a few, could be transformed from analog to digital, and in the process force companies, governments, investors, and citizens to confront a brave new world.

Cryptoassets have exploded in value. Blockchain is the first native digital medium for value, and it's limited really only by our imaginations. We are witnessing one of the largest transformations of wealth in human history. **Value is moving really for the first time from analog assets to digital ones.**

A cryptoasset is a digital asset that uses cryptography, a peer-to-peer network, and a public ledger to do 3 things:

1. To regulate the creation of the units
2. To verify transactions
3. To secure these transactions without any middleman.

Blockchain differs from the Internet in 2 fundamental ways:

1. The Internet was a free utility. Early pioneers built-in with really little financial incentive.
   Bockchain provides potentially huge rewards for creators of widely used platforms and apps. Blockchain creators and early adopters can participate financially, in the growth of the second era of the Internet.
   Because of that there is no one blockchain, there is an explosion of competing, overlapping complimentary platforms, and all are driven by incentives.
2. Blockchain is tackling value industries like financial services and supply chains.

The technology behind cryptocurrencies, blockchain, can work with any type of asset, making it easier to trade, store, and record ownership of basically everything.

Cryptocurrencies

Bitcoin is the workhorse of the cryptocurrency world. It stores it on the most robust computer network ever formed.
It's a secure payment system enabling billions of dollars in transactions daily.
Bitcoin is a reserve currency for the growing cryptoasset world. That means that you can use it as a final settlement when it's time to cash out.
Bitcoin's meteoric rise in price makes it easier, not harder, for new investors to justify buying some. It's become too big to ignore. The bigger bitcoin gets, the more uses it has.
In 2018, the Lightning Network and other scaling solutions were launched. With these, bitcoin may fulfill the promise of its biggest fans and end the need for traditional go-betweens.

The big banks are changing their tune about bitcoin. So bitcoin has already had a huge impact on culture and the economy.

Newer cryptocurrencies like Zcash have emerged and those focus on privacy. These and other so-called privacy coins build upon bitcoins principles but add privacy into the mix.

Another intriguing cryptocurrency is Metronome. It is issued on the bitcoin network as well as on ethereum classic and others. What makes Metronome so interesting, is users can import and export it across chains. Such interoperability is a big challenge but it's also a big opportunity.

Protocol Tokens

Cryptocurrency is design to function as cash for the Internet. That's true when it comes to bitcoin ,but Etherium is different.

Protocol tokens like Ether are connected to a platform like Ethereum.
Ethereum is a blockchain platform to run DApps where DApps is short for decentralized applications. **DApps are powered by smart contract software that automated the logic of a business agreement.** DApps help cut out the middlemen. Bankers, brokers, lawyers and escrow agents are no longer needed really to guarantee the execution of an agreement.
Ethereum is the leading platform for initial coin offerings or ICOs.

Ethereum is, in many respects, the first automated investment bank for the digital economy. And so far, dozens of distributed applications have launched on the Ethereum network. They've raised billions of dollars.

Large enterprises like Microsoft, JP Morgan and BP formed the Enterprise Ethereum Alliance in 2017 to build out this ecosystem. **The network's growing reach gives it some staying power.**

When more DApps are built on a network, demand for the network's protocol token grows. Think of Ethereum as the city grid, and the DApp is the car. Ether is the gas in crypto terms. We pay in ether to use the network for running the smart contract powering the DApp. The more cars on the road, the more demand for gas and the higher the gas price goes.

And significant work is under way to expand Ethereum's capability, including the Casper proof of stake consensus mechanism. A few platforms though are emerging to challenge Ethereum.

Some protocols like the Aion network were built with large scale enterprise applications in mind. This is a huge but generally untapped market still.

Two protocols, getting lots of hyper, Polkadot and Cosmos. They promise to unite all blockchains into a giant seamless web. By allowing different blockchains to operate with each other seamlessly, these platforms would eliminate the risk of building inside a blockchain silos, really only to operate in effect with one single vendor.

Utility Tokens (App Coins)

Utility tokens or app coins are a way for a distributed application to raise funds.

Augur, one of the first projects to hold the crowd sale for utility tokens (ICO), is a prediction market designed to harness the wisdom of crowds in order to make markets in virtually anything.

> Ethereum's co-founder Joe Lubin, believes this new fundraising model (ICO) is democratizing the ability for projects to fund themselves.

Augurs native token is not equity perse, but a utility token that users need in order to interact with the network or the application.

> Lubin says, "A Dapp crowd sale is pre-selling something and using those proceeds to build what you need or to take a project from a rudimentary stage to a more sophisticated stage."

Utility tokens can have applications in virtually every industry. Most ICOs in 2017, 2018 were classified as utility tokens.

Utility tokens are usually not stand-alone blockchains. They typically run on top of platforms like Ethereum, EOS. The distinction between utility tokens and the underlying platform tokens can be a subtle one. After all, protocol tokens also have utility, like the ether that's used to pay transaction fees on the Ethereum network.

Security Tokens

It's right there in the name, securities, security token, meaning digital bearer asset.

Security Token Offerings or so-called STOs are the offspring in many respects of Initial Coin Offerings or ICOs.

In the next 10 years, we'll see today's cryptoassets lose their monopoly as securities like stocks and bonds migrate to this technology and increasingly dominate the market share.
A traditional stock trade can take up to three days to settle, and involves a handful of middlemen. **With blockchain, a buyer and seller can complete the same transaction peer-to-peer on a decentralized exchange on the same day, indeed often within seconds.**
So, why shouldn't all these assets, stocks, bonds, dividends, futures, forwards, swaps, options, and other financial assets, exist in purely digital form on blockchains? This great migration of value from analog to digital is already happening.

> Fidelity, Wellington and other giants of asset management are preparing for this brave new world. There are projects and companies building out the technology infrastructure for what could be a historic transformation, but the regulatory infrastructure still lags behind.

Security tokens can help restore public trust in cryptoassets.

Natural Asset and Commodity Tokens

> Michael Casey, the co-author of the Truth Machine, wrote, "We may be moving towards a model of programmable money, capable of delivering an automated system of internal governance over common resources.”

We can tokenize technology protocols, applications, and even securities into cryptoassets and the same principle can apply to physical assets in the real world.
Entrepreneurs and enterprises have transferred this idea to traditional commodities, with established markets like gold, oil, or natural gas.

> AEON protocol, worked with the TMX group, owner of the Toronto Stock Exchange, to show how it's feasible to copy the business logic of an oil futures contract onto the blockchain. The blockchain can simplify how we clear and settle a trade in an underlying physical asset.
>
> We can also use a token backed by gold as a less volatile and more liquid medium of exchange. Royal Mint partnered with the Chicago Mercantile Exchange to create a digital gold token, backed by actual gold in the Royal Mint's vaults.

So blockchain technology can streamline existing commodities markets.

Now, natural resources are a hard market to penetrate because of the lack of standards and because it's a fragmented audience. Blockchain could change that by aligning incentives with a common goal, like reducing carbon emissions.

> Companies like CarbonX in Canada or Veridium in the United States, are tackling this market by tokenizing carbon credits.

Today, natural asset tokens are a tiny market compared with cryptocurrencies, utility tokens, and even security tokens. It's still mostly theoretical and there are also some real challenges in the form of government policy and regulations.

The underlying market here is massive and untapped. It's only a matter of time before this becomes one of the largest cryptoasset types.

Crypto-collectibles (Non-fungible Tokens, NFT)

Crypto collectibles are means of engaging people with blockchain technology.

> In December, 2017 the crypto world caught crypto kitty fever. CryptoKitties are unique tradable virtual pets. People can buy them, raise them and even breed them with other CryptoKitties. As of January, 2018, CryptoKitties had more than 235,000 users. And it had processed $52 million in transactions, running on the Ethereum network.

CryptoKitties got so popular that Ethereum itself struggled to keep up, which was a sign of two things.

1. popular apps have powerful network effects
2. the underlying platform technology is still currently limited. It can't handle such popularity.

There are two kinds of crypto-collectibles, **virtual and real life.**

1. CryptoKitties and virtual trading cards are native digital assets without a real life equivalent.

   Artists are also applying crypto-economics to their virtual art. Art derives much of its value because it is scarce.
   But the Internet of information let's us copy images and songs over and over, reducing the value close to zero. And loosing track of the original, and who owns it.
   The blockchain connects the creative work to a unique and scarce token.
   More and more, art and other forms of expression are starting out digital. This is an exciting opportunity. Whole new categories of virtual art and collectibles could potentially explode in value.
2. The second kind of crypto-collectible represents a claim on something tangible.
   Virtual art is a growing market, but the existing market is huge. Total sales in 2016 of fine art and antiques was $45 billion.
   A company called Artlery came up with the CLIO, an art-backed cryptocurrency to register real world works of art.

Artwork can get a digital fingerprint through a crypto-asset allowing us to trace, track and verify it.

Crypto-fiat Currencies and Stablecoins

Rogue governments could use their crypto-currencies to undermine international law, treaties, and sanctions. But it also shows something important. Governments can actually do this.

> In 2017, Venezuela announced it was launching a cryptocurrency called The Petro backed by its vast oil reserves.
> According to analysts, Venezuela's Petro already has about three strikes going against it.
> One, there's no evidence that the Petro's actually backed by oil.
> Two, there's little technical information online about how it works or even which blockchain it runs on.
> Three, it's controlled by the same people who tanked the Bolivar.
> Venezuela's government moved ahead ignoring this criticism. It raised $735 million according to its officials. There was no other evidence to back up this claim.

The most promising candidates to establish a government-backed cryptocurrency are respected institutions like The Bank of England, The Bank of Canada, and the Federal Reserve. But they've made little progress or even backtracked somewhat. They should reconsider.

Crypto-fiat currencies probably won't be fully decentralized and resistant to censorship like Bitcoin. But if they implemented in the right way, they can still make markets more efficient through real time settlement, they can improve inclusion by reducing barriers to entry, they can increase transparency into our institutions, and they can make central bank policy more effective and more responsive to events.

Stablecoins are emerging as a hybrid cryptocurrency.
Stablecoins try to maintain the same value over time, almost always by pegging themselves to some underlying asset, like a fiat-currency or gold or by managing price through an ever-changing supply.

> The largest one today is Tether or USDT. Its creators say Tether's back dollar for dollar with US dollar reserves.
>
> With a stablecoin like Tether, you have to trust a single entity who now becomes the monetary authority

Stablecoins could gain traction assuming two conditions.

- First, if existing cryptocurrencies like Bitcoin remain highly volatile.
- Second, if governments don't create their own crypto-fiat currencies.

So stablecoins will continue to be an interesting area of innovation.

Initial Coin Offerings (ICOs)

The term ICO is a bit of a misnomer. **These aren't necessarily coins in the sense of them being cryptocurrencies, but rather digital assets that can represent many things**, such as ownership in a company, access to a network, carbon credits, or even art. A better term would be **Token Generation Events.**

Initial Coin Offerings are fundamentally changing how companies, investors, and users come together.

Now companies can raise funds on the blockchain by issuing tokens or crypto-securities. These can represent equity in the company or even bonds.

> A project called Augur launched one of the most successful crowdfunding campaigns ever. In the first week, more than 3,500 people from the United States, Asia, Europe, South America, and Africa contributed a total of four million dollars to the project. There was no brokerage, no investment bank, no stock exchange, no mandatory filings, no regulator, and no lawyers, not even a Kickstarter or Indiegogo.

ICOs are paving the way for a new type of distributed virtual exchange, and even bigger success than Augur was Ethereum. It funded the development of a whole new blockchain, through a crowd sale of its own named Ether. In 2014, when Ethereum raised around $20 million, it was the largest crowdfunding initiative ever.

There are reasons to be optimistic, that the creation of this new funding model will mean entrepreneurs anywhere can raise funds and support the growth of a new business.

Smart Contracts

Introduction to Smart Contracts

> Smart contracts are the brainchild of **Nick Sczabo**. He's a computer scientist, a legal scholar, a cryptographer. He came up with the idea of smart contracts back in the early 1990s. Also in the 1990s, Nick came up with the idea of digital gold as he called it. So, he's considered one of Blockchains pioneers, for this foundational work.

Blockchain-based smart contracts helped to do three things.

1. They reduce transaction costs by eliminating the need for intermediaries.
2. They improve the security and the privacy of the parties involved.
3. They help to enforce the terms of an agreement.

What Are Smart Contracts?

> Contracts are part of the basic building blocks of our identity, our global economy and for that matter, society at large.
> Contracts set mutually agreeable rules, the terms of conditions for assets and performance incentives in the form of rewards and penalties.

Smart contract is a new concept in both law and in finance. **It's software coded to mimic the logic of an agreement.** It has a unique method of ensuring compliance, namely, it can automate performance.

A smart contract can call an algorithms and sensors to decide whether the agreed upon conditions have been met, program it into a specific control structure. This structure let you predict the contracts outcome at any point in time. **What's key is, the contract can't be seized, or stopped, or redirected to a different Blockchain address, once it's set in motion on a Blockchain.** No central authority or third party can revoke it. No one can override the consensus of the Blockchain Network. All you have to do, is transmit the sign transaction to any of the blockchain network nodes, and this can happen from anywhere using pretty much any medium.
Let's say someone shut down the Internet, or a government agency tried to stifle communication. You could still conduct the transaction whether over satellite or shortwave radio with Morse code. All you need is someone on the other end to decode the deal and record it in the Blockchain. It's provable with mathematical certainty.

> Nick Szabo, the father of smart contracts, compares it to an old fashion vending machine. The simple nature of the business relationship is already programmed into the machine. Let's say the machine is selling certain beverages at certain prices. The buyer selects the beverage, inserts enough coins to cover the price. The machine then verifies the amount, dispenses the chosen beverage and makes change if necessary.

Benefits of using larger scale and more complicated smart contracts:

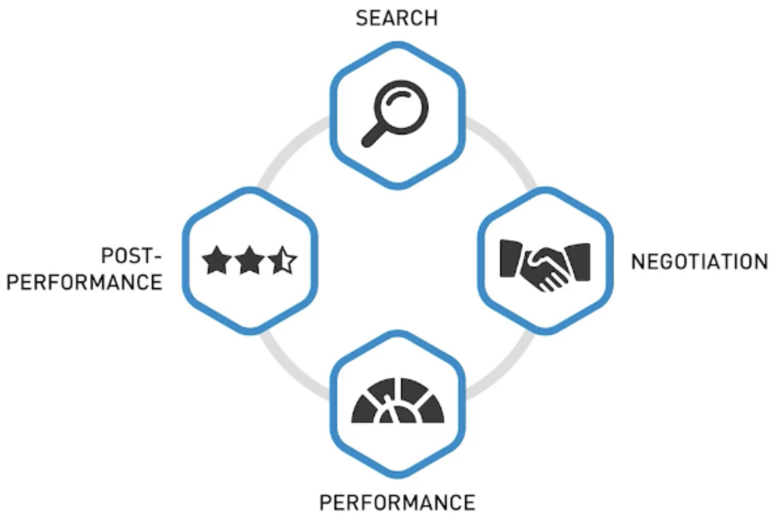
1. Reducing mental transaction costs.
   It means the computer does more precisely and more aptly, what the human mind cannot or prefers not to solve.
2. Increased predictability.
   Smart contracts are mathematical. They're enacted by machines distributed across a Blockchain Network. This enables us to measure loss and manage risk more accurately. This is especially useful in financial or legal areas, or uncertainties can be high.
3. Broad security
   We need to think about the security of all aspects and functions of our business relationships.
   Traditional contracts tends to leave security holes and are disconnected from actual control over assets. Smart contracts directly control those assets and they can provide far ranging security in our business dealings.

You may wonder if they're legally binding.
There is no final answer yet.

> Under US common law, parties can express or imply an agreement. They needn't draft nor sign a paper contract for the terms to be legally binding.
> Legal scholars Primavera De Filipi and Aaron Wright, belief smart contracts honoring legal agreements, are likely enforceable under US law. Intent will be expressed through code rather than through paper.
>
> If the obligations are recurring, then smart contracts, could even serve as protocols of performance. Only time and courts around the world will tell.

Smart Contract Phases

Blockchain-based smart contracts may spar the next economic revolution by transforming these phases.



The search phase
The phase when buyers and sellers find and size up each other.
The first era of the Internet was great for search, new web browsers and search engines, allowed people to connect and to find each other all around the world.

The negotiation phase

It is the process of agreeing upon and committing to deal terms.

The performance phase

It ends when the terms of the contract have been performed.
Ensuring performance involves managing collateral. Collateral can be money, a guarantee, or a product.
In the first era of the Internet, few innovations have occurred in this phase. Compared to past decades, automation has increased proof of performance with advancements in computers, sensors, and blockchain technology.
But the pace of this progress pales in comparison to the gains made in the search and negotiation phases.
In this phase, the smart contract manages the collateral. It can hold it in escrow and either free it or cease it to effect an outcome. That barely scratches the surface of smart contracts capability in this performance phase.

Post-performance incentive phase

It’s used to ensure the desired outcome. These include chargebackability, ratings, and contract law.

The point of smart contracts is to reduce reliance on litigation.

Computers and the Internet have made ample innovations in this phase.

By applying this technology to all four phases. **Smart contracts have improved in security, integrity, and they enable globally seamless reach.** We need to support more kinds of deals between increasingly far-flung and differently laude and cultured people, and deals between devices on the Internet of Things as well.
Cryptocurrencies, tokens, blockchain-based smart contracts can create value by permitting continual money storage and transfer in the performance phase.
Second layer or peripheral networks like lightning will help us use this currency in settlement systems for payments at a larger scale too.

Smart Vs Traditional Contracts

Traditional Contracts

Logic, in traditional law, stems from the minds of people and their analogies. Traditional contracts take the form of human language, interpreted mainly by lawyers. It's very flexible, even corruptible. It involves human judgment, it lives in jurisdictional silos, it's very local, and it's very nationalistic.

> Nick Szabo, the father of smart contracts calls this traditional contract language, **wet code.**

Traditional contracts tend to be biased towards their jurisdiction of origin.

Smart Contracts

Software relies on bits, data, and Boolean logic. It's rigid and it's predictable. It runs the same on every computer, on the network, anywhere in the world.

Smart contracts, contain rules and conditions analyzed by software code. Along with the code, performance is verified and executed by impartial technology, such as sensor guided effectors. We call this kind of contract language **dry code.**

The main task of software engineering, as well as contract drafting, is to **anticipate the behavior of parties and related events in their performance.** The more anticipated cases, the more conditions, and the contract.

In dry code, each condition increases the complexity and attack surface of the code. Attack surface refers to the number of points in the software program, where an attacker could break in or takeover any assets controlled by the program. If the program is a smart contract, the assets could be your digital identity or your private data, or your crypto-assets, important stuff. **More conditions usually increase the contracts reliance, on potentially imperfect or external data.**

Dry code can yield harsh results if the coder is overlooked the scenario. It would take some rewind capability and what's called multiple signature authority or multisig for short, for the two unhappy parties to reverse the outcome. Otherwise, the results may be hard to undo, without traditional legal intervention.

Blockchains apply the same rules everywhere on the globe.

Working together, wet code and dry code can secure the foundation for strong business relationships. Lawyers don't need to worry about robots taking their jobs, their work complements the work of machines, running smart contracts.
Smart contracts are part of the digital evolution of deal-making in contract law. They make possible what was once impossible. That's why lawyers and software engineers need to break out of their silos and work together. Lawyers can learn the basics of coding, and engineers can learn the basics of contract language. They can together run deal scenarios, and then work out the terms and conditions of the deal together.

Smart Contracts and Law

A smart contract is a set of security protocols taking on the burden of lawsuit. A smart contract like a repo man adds a layer of security. This layer can match the rights and requirements expected from a relationship with concrete action. Running on a public blockchain, smart contracts can control assets jointly with authorized addresses namely, public key pairs controlled by users.

In other words, smart contracts may reduce the need to seek remedy with traditional law.

Smart contracts make some cross-border relationships between small businesses and individuals possible by reducing the reliance on complex and outdated methods.

Will smart contracts hold up in court?

A smart contract generally makes no attempt to be legally binding. It's called a smart contract because it mimics or improves upon the effects of a traditional legal contract. It provides incentives for performance, not by threatening litigation but by using software to control money and other assets.
If the smart contract can't take into account all probable factors and the risk of a lawsuit, then a traditional contract may also be needed. In such cases, it's risky to expect the parties, lawyers, judges, and jurors to interpret the dry code. That is, to decipher the lines of software code. They'll need to look at the wet code like the user interface and the traditional legal texts that lawyers use. We may need to supplement our dry code with wet code evolved from lawyers of the jurisdiction. The cost will be high but then again, so is the risk without it.

What if the execution of the smart contract penalizes one party too harshly?

Most likely, it'll take the traditional system to fix the problem, and that could be costly. So, we may want to supplement traditional contracts with smart contracts. Both parties have the option to roll back undesired, unexpected outcomes.

There are some smart contract programming options available to deal with contract breaches. One is **performance verification code.** It detects a failure in execution. It will seize the on chain collateral of whoever breached the contract as payment for damages. If the outcome is unsatisfactory for both parties, then they can rewind some of their transactions through the **multi-sig rewind.**

Smart Contract and Regtech

Smart contracts are not regulatory technology (Regtech). Smart contracts are global and persist on a globally distributed blockchain. They're specific to the dry code as programmed by their original coders. They control assets and verify performance obligations. So, they manage the burden of lawsuit.

Regtech is about checking whether human beings are complying with laws and regulations in certain areas. Regtech is only a simulation of how wet code may be enforced by a court.

Smart contracts deal with assets. They don't have knowledge of all of the world's legal systems. Regtech focuses on the application of wet code. These two forms of technology are clearly different at this stage in the evolution of blockchain technology.

Smart Contract Application Areas

1. **Retail Payments**
   The implementation of blockchain-based smart contracts may be just around the corner. Smart payments could revolutionize the whole payment system.
   But using them on a public blockchain poses a challenge at the moment. Public blockchains can't get scale to very large volumes, at least not without taking up massive amounts of network bandwidth. Because of this, full nodes could fail to provide security and compromise the network.
   Second layer or peripheral systems, like lightning for Bitcoin or Sprite or Raiden for Ethereum could solve this problem. These run in smart contract fashion by posting collateral on the public blockchain. The collateral ensures a long series of off chain transactions will finally reach settlement on chain without using excess energy.

2. **Worry-minimized commerce**
   Consumers want simplicity, and that starts with the deal funnel. Our perspective customers enter the funnel when they find us. They come out the other end as full fledged customers, when both of us have performed our parts of the deal. In between those points, the deal funnel narrows. **For whatever reason, we tend to lose most prospects as they move through the process. The key is to lower the index of worry for customers.**

   Worry-free commerce is like using a vending machine, you stick the money into the machine, your soda comes out, transactions complete. You don't want to keep adding money hoping some amount will finally get you to soda. Likewise, consumers and other industries don't want the hassle of repeated actions and added charges, sacrificing their limited time, or their private information is not always worth the product or service could be received.
   One way to change this is by shortening the forms that customers must fill out. The fewer lines on the form, the less exposed or

at risk customers feel. There's also the fear of overcharges for services with no set value. If we can reduce customers worries about cutting forms and recurring charges, then the drop off rate should decrease.

How do we do this?
First, we get rid of advertisements and those payment windows fulfilling out and saving credit card information in some centralized database. That includes, the databases of payment processors like PayPal, Square, and Spotify.
Then we implement a blockchain base payment system. This system never ask customers to enter confidential information, and never stores such information.
We're talking about a second layer retail blockchain solution. Such a solution could greatly reduce these consumer worries. They could shorten their process, and at the same time have their privacy protected.

3. **Insurance (with parametric contracts)**
   A parametric contract pays out based on measurable data not on some estimate of the loss. This means that, assesses the actual loss and revenue following an insured event. Specifically, it uses an input oracle tested for yielding quality data, and this oracle monitors the insured parties books for actual revenue losses.
   Parametric contracts are far more open to smart contract automation. They need fewer manual steps, if any at all.
   Traditional insurance depends on claims adjustment usually based on subjective or qualitative data.
4. **Logistics**
   Smart contracts could improve logistic systems across a supply chain, especially across boundaries where parties may not know or not trust each other.
   They could optimize supply chain logistics, from the machines, making the parts to the parts themselves, track from the factory floor to their final usage. This is possible through the combination of communication networks, the Global Positioning System(GPS), scanning and sensor technology and the Internet of Things. Participants could track assets by their barcodes as they pass through physical checkpoints like ports or warehouses. **Smart contracts would identify performance as the assets move through time and space. They trigger devices like sensors to hash data on their whereabouts, onto a shared blockchain.**
   We could speed up the metabolism of supply chains, and we could improve inventory management, transportation, distribution, accounting, payment processes, and more, across entire deal cycles.
5. **Algorithmic Management**
   If you've ever obeyed a traffic light, then you've been managed by an algorithm. Computers decide when the lights change based on sensors in the pavement, monitoring traffic flow, and so on. Algorithms decide when we must stop, and when we may go.
   In employment situations, where performance can be measured, computers can keep track of far more people than human bosses can, and with greater detail, well, perfect memory. We think of algorithmic management as involving employees, but these capabilities could also foster new relationships. The ability to specify a task and verify its performance, this may lead to more hiring of independent contractors, for example, less hiring of employees on a payroll.

Smart Contract Strategies & Best Practices for the Organization

Five of Nick Szabo’s suggestions for deciding whether blockchains and smart contracts can help you in business.

1. **Audit your organization's business processes for measurable changes.**
   Look for conditions of performance you could verify by sensors or computers. These could include, payments, financial arrangements, logistics, checkpoints, and tasks involving time, and distance. You could use smart contracts with oracles in these cases.
2. **If you're coordinating activities across borders, consider using public blockchains rather than private ones.**
   The security of public blockchains depends on computer science rather than on local law enforcement. That makes them more reliable and less susceptible to human interference or worse corruption.
   Mature public blockchains are securely permission-less and seamlessly global. Those qualities make them more secure and reliable under a whole variety of conditions be they local, regional, or international. They also help you expand your global reach.
3. **If you'd like to reduce your need for intermediaries for verifying identity or adapting to local laws.**
   Make your business processes less like a bureaucracy both internal and outward-facing. Make them more like a vending machine. That means few to no forms to fill out, more metrics to call on and respond to. You're not imposed the risk of identity theft on your stakeholders as lots of other organizations impose on theirs.

You'll also reduce your legal risks. You may even increase your reputation as a stress-free, worry-free party to do business with.

4. **Consider hiring lawyers who know computer science, and software engineers who know law.**
   Ask them to collaborate on codifying the basics of your business relationships. It's important for your lawyers and software engineers to know the strengths and weaknesses of each other's approach. Software engineers will benefit from knowing the history of contract law and practice.
5. **If you'd like to shrink payroll and increase your business flexibility, then consider converting some or all of your employment contracts into independent contract or business outsourcing contracts.**
   If you can verify performance of certain employee tasks with measurement rather than human judgment, then this could work for you.
   It allows you to outsource more tasks as you need them completed, measuring performance, stresses, best practices. It also opens up competitive bidding for those tasks.
   This is especially useful across national borders. Businesses hire employees when contracts can't possibly cover all the tasks that they may need to do or perform. Instead, they assign tasks on the fly. So whoever on staff is available and qualified, gets to do it.
   Once you can codify and measure an employee task, you can restructure your contractual relationship with the person completing it.

Identity

For true freedom, we need self-sovereign identities. Identities we create and control. Identities no one can copy or take from us. Identities where we own and control all the data that we generate.

Strong data governance is essential, and this means managing the incentives for creating and collecting data.

Identity and Identifiers

Introduction to Identity and Identifiers (Identification)

First of all, we believe people have the inalienable right to establish our own identities.
We also have the right to capture and control our own data that constitute these identities.

> That's not the case right now.
> Most of us are generating **data, the new asset class** for big companies like, Apple, Facebook, Amazon, Netflix, Google, Banks, Credit card companies, Governments, the big internet landowners.

The second era of the internet based on Blockchain, will bring about a new economy for data. This new asset class of the digital age. Largely, because **Blockchain technology enables us to establish and own identities.** It **also enables us to enforce these identities in any context**, we can create a virtual Black Box for storing our own personal data.
By creating the virtual you and safeguarding this virtual you through Blockchain technologies. **You can take back control over your own identity. The data you create and all the related rights of privacy, publicity, and property.** We can recapture our identities and manage them for ourselves. To help use this data to plan our lives, to monetize it if we want and to protect our rights to privacy.

Self sovereign means that it's under your individual control. It's also inalienable, meaning it can't be separated from you. No one can steal it, and since it's not assigned by a central authority, no authority can take it away. It must be recognized and enforceable in any context.

Identifiers

Identifiers are simply what we use to participate in large centralized systems like, Gmail. They identify who we are,

Identity

Identities are the whole of us. They're something we experience and reveal to others selectively over time. Y

and we collect a lot of identifiers in our lifetime. Some of them are enduring like a social security number. Others are more transitory and employee ID, Student ID, and some are inherent to us like our fingerprint. Others we select like username or a password and still others are assigned to us, and as we use them, they all generate personal data. **These are not our identities.**

our identity exists before anybody registers your birth on a ledger.
Identity is not simply endowed at birth. It is endowed by birth. But until now, we haven't had a means to assert this authority.

Five Problems with Identifiers

1. **The need for some overarching identifier like a birth certificate.**
   Before we can get an identifier like a social security number or a driver's license, we usually have to show some original record of our existence with our name, our birth date, and so on. It's often a birth certificate, created and verified by a licensed hospital or a licensed midwife. Any copies of this certificate must be notarized to be acceptable as an official record, but getting a birth certificate is actually no small feat.

   UNICEF estimates a quarter of all births go unrecorded worldwide, and not getting a birth certificate can have life shattering consequences.
   The World Bank estimates 1.5 billion people on the planet lack some original proof of existence and that complicates being able to claim status.

   The World Bank has an initiative called Identification for Development. It's designed to help more people take part in the global economy.

   India documented 99 percent of adults. The problem was storing all the demographic and biometric data in a centralized database. The system was hacked and one billion records were exposed. So, the reality of a centrally sourced and government sanctioned identity is a big problem.
2. **Government identifiers are systems-centric, system-controlled, and vulnerable to cancellation, to forgery and even theft.**
3. **All the personal data we create with each identifier is stored in somebody else's central database.**
   That person or that institution may give our data to untrustworthy vendors or sell our data to unacceptable third parties without our permission or even our knowledge. In the meantime, our data keeps flowing to these databases out of our control.
4. **The identifier-centric system is extremely user unfriendly.**
   We have to repeat the registration process whenever we get a new identifier and we provide the same forms of ID.
   We keep portfolios of ID numbers, usernames, passwords and the answers to personal questions.
   Porting data is complicated and the rules often change.
5. **Whenever the central database is hacked, we're left to clean up the mess.**
   We bear most of the risk for our own data but we get none of the rewards of third party data usage.
   Our identities should be informing how we manage our identifiers. Instead, these identifiers are deforming our identities.

Identity on a Blockchain

Distributed, Self-sovereign Identity Systems

By letting whosever in charge of the government control our identification, there's a case to be made that we're giving them way too much power over our personal lives. It's too risky.
We should be controlling our own identities, free of the country we're born in or where we reside.

Identify Commons

Identify commons, it's important for all users to have the right to manage their own identities. And that includes making money from their own data. That means controlling who has access to it, and that means making the rules over how to preserve and use the commons.

This identity commons needs four qualities:

1. **It must be free of any corporate or government or other third party and their control.**
   That way, it won't be subject to the winds of some large central authority.
   It still needs to be able to work with these parties, of course.
2. **It must outlive us users so we can transfer our assets to our heirs.**
   Maybe we can will our data, such as medical records, to our heirs.
3. **It must enforce the right to be forgotten.**
   On a practical level, that means **separating data rights from the actual data** so data rights holders can delete them.
4. **It must be inclusive so that everybody can use it.**
   That means the system must be user friendly, with a low-tech mobile interface and low-cost dispute resolution.

The technical groundwork has already been laid, public key infrastructure(PKI). Blockchain separates the identification layer from the verification layer in a transaction.

Blockchain’s privacy is by design.
Zero-knowledge proofs, where minors can validate transactions and bundle them into a block with zero knowledge about their details. And this is an enormous innovation, it's a system for verifying the truth without knowing what the truth is or who it involves.

Blockchain Identity Applications

Blockchain users can already obtain digital identifiers through a variety of startups.
They can use Civic, ShoCard, uPort and the Shyft Network, etc.

Example: uPort

It's identifier has a unique and persistent 20 byte hexadecimal string at its core. Hexadecimal is a number system with a base of 16 symbols. The position of these symbols has meaning in math and in computer science. This hexadecimal string serves as the address of a specific type of smart contract called a **proxy contract**.

The proxy contract lets us sign and verify a transaction, an action, or a claim. They also help us manage cryptocurrencies and other tokenized assets.

Proxy contracts can interact with other smart contracts on the blockchain. They can also link to our off-chain data, and grant others temporary permission to read or write one of our data files.

The uPort system works for devices such as driverless cars or 3D printers, those things need identities too. uPort also interacts with virtual entities, like IBM's Watson, and institutions, like banks. Finally, uPort has a mobile app for cryptographic keys, just for our convenience and security.

Another type of smart contract is the controller contract. **A controller contract separates our cryptographic keys from the proxy contract. It contains a logic for identity recovery.**
This means basically, if your device is lost or stolen, you can replace your private key without having to replace your proxy identifier and all the assets that are associated with it.

Example: Shyft

Shyft is a blockchain based network compliant with know your customer and anti-money laundering regulations in the financial world. It helps users who are managing and working with data to be regulatory compliant.
Shyft reduces the costs of compliance and it increases data security. It protects identity better than traditional compliance systems.
Blockchain makes regulatory compliance cheaper, faster and more secure.

Decentralized Identity Foundation

It's a consortium consisting of Hyperledger, R3 and Sovrin, as well as more established companies, like Accenture, Microsoft and IBM. This consortium is dedicated to creating the identity commons. It uses decentralized identities, blockchain IDs and zero trust data stores.

The consortium focuses on three big areas:

1. identifiers and discovery
2. storage and computation of data

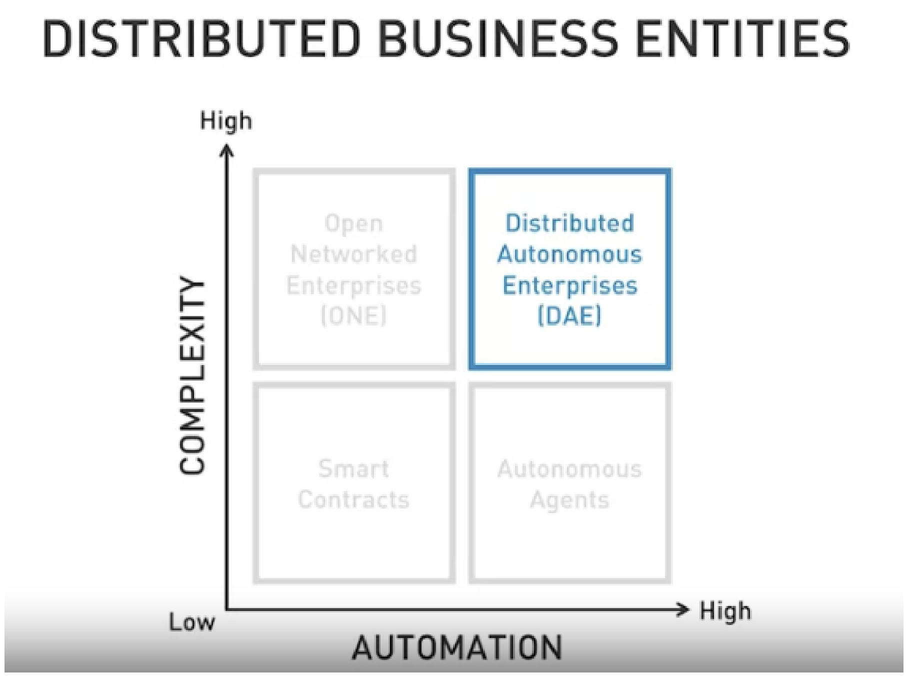
3. attestation and reputation.

The consortium's long term goal is to develop use cases and standards for identity management.

> **Fabian Vogelsteller,** the father of the distributed application for initial coin offerings is also working a distributed application for identity.
> In 2017, he issued Ethereum Request for Comment, Issue 725, abbreviated as **ERC 725**.
> If his standard takes off, as his standard for initial coin offerings did, we'll make real progress toward an identity management system that we can all use.

DApps and Distributed Business Models

Distributed Business Entities


DISTRIBUTED BUSINESS ENTITIES
High
COMPLEXITY
Open Networked Enterprises (ONE)
Distributed Autonomous Enterprises (DAE)
Smart Contracts
Autonomous Agents
Low
High
AUTOMATION

Some of the new and very radical and very distributed forms of businesses that could be made possible by blockchain technology.

These types of businesses need little or no traditional managers to create value for customers and owners.

Millions of people could collaborate and ventures like these and share in their profits. The result will distribute wealth to many instead of keeping it for the few at the top of a hierarchy.

Smart Contracts can go from the simple to the complex. Simple contracts involve few or no people.

Complex contracts call on more people and involve many exchanges making firms resemble networks. We call these **Open Networked Enterprises (ONE).** These open networked enterprises are good at coordinating resources anywhere in the world.

Take smart contracts as a step further. Create them as **Autonomous Agents**, make them super smart having machine learning built into them, and pursuing our goals and making decisions on our behalf. This is where blockchain meets artificial intelligence. Artificial intelligence is not going to run on some massive supercomputer centralized in the world somewhere, it will be distributed in autonomous agents running on blockchains.

So imagine a piece of software capable of learning and adapting, roaming on this platform with its own wallet. The software is an autonomous agent in that it can take end data from its environment and act on that data independently. The autonomous agents are more than just computer programs. They can modify how they do their work over time.

More complex agents can make more complex transactions. They could acquire resources or produce value for their owner. It can begin to do things that it wasn't programmed to do. In the future, Autonomous Agents will collaborate forming all kinds of new business models, in what we're calling a **Distributed Autonomous Enterprise(DAE).**

Imagine a set of autonomous agents cooperating in a complex blockchain based ecosystem. They could be coded according to a clear mission statement and operating rules. People will give these agents computing power and capital. Together they'll create a suite of services and sell those services to other devices or to humans, or to human organizations.
They'll buy what they need, hire or require resources like manufacturing or marketing resources, could be equipment or people or services, and they'll adapt in real time. This would be the ultimate distributed organization.
Ultimately, it could have millions of shareholders who participated in a crowd funding campaign to create it. The shareholders having crafted the mission statement would vote to govern the entity, much of the day-to-day decision-making could be programmed.
In theory, this entity could run without traditional managers or managers of any human kind. There would be no overpaid CEO or bloated bureaucracy. There would be no what's called moral hazard where managers do things that are not in the interest of the shareholders and stakeholders of a corporation. There would be no office politics, no red tape. Any human employees or partners would be paid under smart contracts. Smart contracts would run according to the best management practices. People would always know what they're supposed to be doing and have clear performance metrics which would be transparent. The enterprise would be able to apply customer feedback more quickly based on logic. Shareholders would get their share of profits based on real-time accounting and the rules of the crowdfunding campaign.

In theory, we could design a corporation without executives, just shareholders, money, and software. Code and algorithms could replace the executive board with shareholders in control. This structure would have some obvious challenges. There needs to be mechanisms to quickly achieve consensus, and we'd need mechanisms to determine legal liability for company actions

The DAO: A Cautionary Tale

A software startup named Slock.it designed a Smart contract on the ethereum network. The developers called it the **DAO for Decentralized Autonomous Organization.** The DAO was in essence a decentralized investment fund. Its developers promised that it would operate with the iron will of unstoppable code. Fundraising came first. Users could purchase DAO tokens by sending ether to the DAO Smart contract, then token holders could vote on which projects to fund out of the proposals that were submitted. Token holders would get a share of the DAO's holdings. Anyone who disagreed with the funding decision could trigger a split function, moving their funds into a new child DAO.

The voting process itself was flawed and some curators called for moratorium to adjust the problem. However, there turned out to be a even more serious flaw in the DAO code, and ultimately, it would lead to the DAO's demise. An attacker used the flaw to drain funds by calling on the split function available to token holders. The attacker was able to, in essence, withdraw funds over and over without updating the account balance held in the DAO. The attacker funneled a third of the ether raised into a child DAO, where it had to sit for three weeks per the terms of the DAO.

The ethereum community had to decide how to respond. They can do nothing and let the attacker keep the funds or they could change the protocol. Ethereum developers had two possible fixes, both tough choices.
One was a Soft fork. Blacklisting the child DAO, so the funds could never be spent.
The other was a Hard fork, transferring the stolen ether into a new withdrawal contract where token holders could claim their funds. Both fixes were controversial.
The Soft fork was considered a form of transaction censorship, and a security review showed it would create a new vulnerability. So Hard fork was really the only solution, but it meant admitting the ethereum blockchain could be altered or appended.

A key lesson was that **effective blockchain governance requires both on-chain and off-chain mechanisms.**
The DAO showed the limitations of on-chain governance. Managed only by the rules coded into the network, and the Smart contracts that were running on top of it. People also influence its operation off-chain on discussion boards such as on Reddit.
It took a combination of these efforts to address the DAO attack.
The DAO's inventors said the DAO operated according to Smart contract code on the ethereum blockchain. The token holders and curators made the decision about the actions the DAO could take.
The automation within the DAO couldn't replace the human side of governance.
Developers will introduce changes to a blockchain protocol to improve the networks function or to fix technical issues. But some updates have been motivated not by technical reasons but by economic ones.

These incidents force us to rethink blockchain governance. **Internal on-chain governance is not enough.** We can set specific rules and Smart contract code, but we can't guarantee that these rules will execute as intended, and events could make the rules obsolete. So a mechanism is needed to update a blockchain protocol, and stake holders decide that it must be done.

New Business Models

Distributed models will disrupt centralized ones, because they innovate better, they create value at lower cost, and producers can share in the wealth.

Open Networked Enterprise Business Models

The open distributed business models show radical potential to supercharge innovation and create value for shareholders, customers, and societies as a whole.

Blockchain Co-operative

It's formed by people coming together to meet common needs. **This is an opportunity to create a true sharing economy, where individuals and organizations work together as a cooperative and receive most of the value that they create.**

Most of the so-called sharing economy companies like Uber, Airbnb and so on, are really large scale service aggregators and distributors. They aggregate services and they round up suppliers with excess capacity on a centralized platform. Could be cars, lawn equipment, vacant rooms, handyman skills. Then they resell them collecting fees, and creating valuable data about both sides of the exchange, the suppliers and the consumers. They've monetized everything from spare bedrooms and family cars, to underemployed talent and people without full-time jobs.

Blockchain technology can displace some of the matching and accounting functions performed by platforms like Uber.

Creators of Intellectual Property

There are a lot of people in our economy that create value and aren't fairly compensated for it. Blockchain can help.

The annual art market is worth $67 billion. It's a business controlled largely by expert middlemen with access to restricted databases.
The Bitcoin based startup, Verisart is creating a public database of art and collectibles. Its goal is to serve artists and collectors, as well as curators, historians, art appraisers, art insurers and so on.
With Verisart, we can record and track the provenance of any physical or digital work of art. Users can use their mobile device to check works authenticity, its condition, its chain of custody.
Verisart founder, Robert Norton, believes the art world will embrace this decentralized model and a decentralized ledger.

Peer-to-peer Production

Peer producers brought us open source software and Wikipedia. Community members take part for fun to network or because of their beliefs. Blockchain technology can improve their efficiency and reward them for the value they create through incentives and reputation systems.

Sustaining volunteer communities long-term can be challenging though. There's no economic incentive for good behavior. Incompetence and sabotage can cause problems, and trolls, post inflammatory, incorrect or off-topic messages sowing discord. **Blockchain technology discourages bad behavior in these communities. Peers develop reputations for valuable contributions.** Peers could share in the values that they create for corporate-owned communities getting paid through smart contracts.

Linux, nobody owns it but it's the world's most important operating system today. The Wikimedia foundation owns Wikipedia. The Mozilla foundation owns the Firefox web browser. They're now experimenting with blockchain technology.

Peer production can also occur in the purely private sector.
Sometimes a corporation acts as a curator. Readers create the content on the Reddit discussion platform but they don't own the site.
Well, Reddit could benefit from moving to a model where great contributors are rewarded and bad behavior is penalized economically. Consensus is already working on a blockchain alternative to Reddit. The Consensus team thinks financial incentives can improve the quality of conversation without centralized control or censorship.

Companies can also tap into vast pools of external labor.
IBM embraced the Linux community donating hundreds of millions of dollars worth of software. Why would they do that? Well, they save $900 million a year developing their own proprietary operating systems. IBM also got a platform on which it built a multi-billion dollar services business as well.

The Metering Economy (metering of asset usage)

This is a different take on the sharing economy. **Renting our excess capacity for all kinds of things** on the Internet of Things.

Renting things like WiFi hot spots, computing processing power, storage capacity, extra mobile minutes, or our remaining battery charge. Your energy sources can become sources of income metering their use and charging the user for it through micro-payments.

All you need is a decentralized protocol for them to transact safely and securely. You decide how much access to allow and what to charge for those rights. Blockchain will meter time and energy usage and manage payments and transactions in real-time.
Owners can pool their resources and then track will stands by their commitments, and those who don't will lower their reputation score and could even lose access if they don't do better.

The Platform Builders

These are business models based on letting anyone use their technology platforms to create value.
Companies can use the power of blockchain programming languages and payment systems to create open platforms, or industry members can partner to create a blockchain utility.

We've used the word prosumer to describe consumers who produce. They hack products to create something new. Blockchain technology supercharges prosumption.
Open platforms could transform entire industries like financial services by settling all kinds of financial transactions. An alliance of big banks is already working on that idea.
Firms use services like InnoCentive or Inno360 to find the right temporary talent to address critical business challenges. It's about using data to find the right talent at the right time to hack your business for the better.

Animating the Physical World

Making things come alive on a blockchain.
Manufacturing-intensive industries though can use blockchain to source, design, and build better physical goods. The technology can also track the origin of goods and their movement through a supply network. Consider the food industry. Smart database management would allow even the largest meat producers to guarantee quality and safety.

Enterprise Collaborators

Commercial collaboration tools within a business are changing the nature of knowledge work and of management inside organizations.
Products like Jive, IBM Connections, Microsoft Outlook, Salesforce Chatter, Google Apps for Work are improving performance and fostering innovation. The social software can transform business operations from human resources and product development to marketing, sales, and customer service.
While blockchain takes today's tools to the next level, existing vendors should face disruption or embrace blockchain technologies to deliver more powerful features.

Think Facebook but for the corporation, where every user has a multi-functional wallet and a digital ID for the decentralized online world. The wallet stores personal and professional data and valuables, including money, but you own and control it.
You hold your pair of public, private keys. The system delivers a stream of valuable information like a colleague's patch of code, a Twitter feed from a conference you missed, a live stream of a client using your new product, photos of your competitors' booths at a industry expo, or help in completing a patent application. You or your firm will gladly pay for this stream. There's advertising, but you, not Facebook, get rewarded for paying attention. That's called an attention market. You can participate in or create discussion channels about important topics.

Companies are adapting into networked organizations, taking advantage of outside capabilities. These collaborative platforms can help enterprises establish trust with their external partners.

DApps

Distributed applications(DApps) represent a new era in the digital revolution with promise for distributing wealth.
DApps are a new level of digital evolution

> *Centralized organizations have held concentrated computing power for a long time. The software markets specialized as the personal computer or PC matured. Some focused on developing client apps for the PC. Some focused on server apps for the host computer. Widespread adoption of the internet allowed individuals and companies to use their computers to share information. Sharing began to democratize the information landscape, but it was short-lived. A new type of timesharing appeared in the 1990s, first called virtual private networks, or VPNs, and then cloud computing. Cloud computing let users and companies store and process their software and data in third party data centers. There are red flags created by the centralized structure. Single points of control make companies and their customers vulnerable to catastrophic crashes, fraud, and security breaches. Systems of different parts of a company still have big challenges communicating with one another, let alone with systems outside the firm. For us users, it means we've never really had control, other people and companies define the services that we use and sometimes they're implicit values and goals are in conflict with our own. Other people own the valuable data we generate, and they're using it to build vast fortunes perhaps the greatest in history. Most of us get little benefit or compensation for handing over our data. Central Powers use it to sell us stuff or to spy on us.*

Then along came blockchain and distributed applications. Now, anyone can upload a program onto the blockchain and leave it to self execute with the strong guarantee that the program will continue to perform securely.
This platform is public not inside an organization and it contains a growing set of resources like digital money to reward and promote certain behavior. We're moving into a new stage of the digital age where we can program and share distributed software.
A distributed application, or DApp runs across many computing devices, not on a single server. All the computing resources running a particular blockchain make up a computer. Critical rules are built into the computer to protect its integrity.

> Blockchain developer Gavin Wood makes this point too in describing the Ethereum blockchain as a platform for processor. He said, "There is only one Ethereum computer in the world. It's multi-user. Anyone whoever uses it is automatically signed in.”

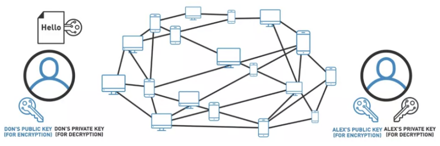
> BitTorrent, the peer-to-peer file sharing app came along even before blockchain, but its distributed nature shows the potential of DApps. At one point, it consumed over five percent of all internet traffic. Lovers of music, film and other media use it to share their files for free with no central server for authorities to shut down.

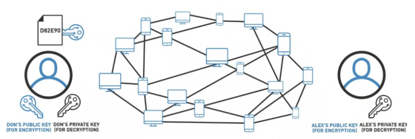
An example: bAirbnb (brainstormed blockchain airbnb)

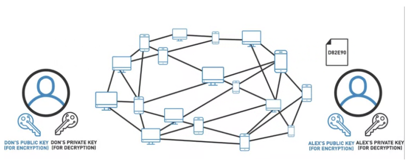
Airbnb become a $31 billion platform, now the world's largest supplier of rooms measured by market share, value in rooms occupied. But the people who provide the rooms get just part of the value they create.

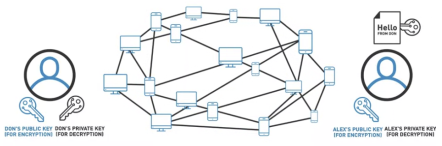
Companies like Airbnb are part of the so-called sharing economy. But Airbnb is not really successful because it shares, rather it is successful because it does not share. It aggregates excess capacity through a centralized platform and resells it at a profit pocketing fees. But more importantly, owning the platform outright.

Now, imagine a competitor to Airbnb but on the blockchain. We brainstormed with blockchain expert Dino Mark Angaritis to design one. We called it bAirbnb.
It would look more like a member owned cooperative than accompany. All revenues except overhead would go to its members. They would control the platform and they would make decisions. bAirbnb is a distributed application. A DApp. A set of smart contracts on a home sharing blockchain.


Hello
DON'S PUBLIC KEY (FOR ENCRYPTION)
DON'S PRIVATE KEY (FOR DECRYPTION)
ALEX'S PUBLIC KEY (FOR ENCRYPTION)
ALEX'S PRIVATE KEY (FOR DECRYPTION)


D82E90
DON'S PUBLIC KEY (FOR ENCRYPTION)
DON'S PRIVATE KEY (FOR DECRYPTION)
ALEX'S PUBLIC KEY (FOR ENCRYPTION)
ALEX'S PRIVATE KEY (FOR DECRYPTION)


D82E90
DON'S PUBLIC KEY (FOR ENCRYPTION)
DON'S PRIVATE KEY (FOR DECRYPTION)
ALEX'S PUBLIC KEY (FOR ENCRYPTION)
ALEX'S PRIVATE KEY (FOR DECRYPTION)


Hello
FROM DON
DON'S PUBLIC KEY (FOR ENCRYPTION)
DON'S PRIVATE KEY (FOR DECRYPTION)
ALEX'S PUBLIC KEY (FOR ENCRYPTION)
ALEX'S PRIVATE KEY (FOR DECRYPTION)

The platform keeps reputation scores of owners and renters to improve everyone's business decisions. So, you're looking to rent, the bAirbnb software filters the listing meeting your criteria. Your user experience is identical to what you would get in Airbnb or at least very similar, except you communicate peer-to-peer on this network through encrypted messages, not stored in Airbnb's database. You and the room owner are the only two people who can read these messages, and you can swap phone numbers and complete that exchange privately. Y**ou and the owner could complete the transaction entirely off chain, but there are several advantages to doing it on chain.**

1. **Reputation**
   The **network** records the transaction on the blockchain. A positive review improves each user's reputation. The risk of a negative review motivates hosts and guests to be honest. People with good reputations can benefit from the same persona across multiple DApps. **It doesn't have to be isolated to just one function.**
2. **Identity Verification**
   We're not dealing with a centralized system to check ID for us. So hosts and guests need a way to confirm each other's real-world identity. The blockchain **calls up a contract from a verify ID application** to verify each party's public key or persona.
3. **Privacy Protection**
   Verify ID application doesn't store all transactions in a database. It's simply returns a true or false to verification requests. Different kinds of DApps can use this verify ID. But verify ID never knows transaction details. **This separation of the identity layer from the transaction layer greatly improves your privacy.**
4. **Risk Reduction**
   On Airbnb, customers' identities and financial data are stored on centralized servers. These can be hacked and leaked, exposing owners to liabilities. But **there's no central database to hack on the blockchain. There are only individual peer-to-peer transactions.**
5. **Insurance**
   On bAirbnb, **owners can get the bAirbnb insurance DApp.** Renters with good reputations get lower rates and don't have to subsidize renters with a negative history.
   Here's how this could work. You submit a booking requests and bAirbnb sends your public key to the insurance contract for a quote. The insurance DApp contacts list of trusted providers. Insurers perform their own calculations in real-time through an autonomous agent.
6. **Payments**
   Funds are transferred to the owner in seconds, whereas on Airbnb it would take days.
   Owners can also manage security deposits better with smart contracts.
   Some parties use Escrow accounts to release payments nightly, weekly, hourly or in full as the parties agreed. Parties can call for arbitration even in cases of dispute.
7. **Secure Access to Property**
   A Smart Lock connected to the blockchain knows when you've paid. Your near-field communication enabled smartphone can sign a message with your private key as proof of payment when you arrive, and the Smart Lock will open for you. **Owners don't need to drop off keys or visit the property** unless they want to say hello or maybe address some emergency.

You and the owner have now saved most of the fees. Settlements are assured and instant. There are no foreign exchange fees for international contracts. You don't have to worry about stolen identity. Local governments and oppressive regimes can't subpoena bAirbnb for its rental history data. This is the real sharing and value economy. Both customers and service providers are the winners.

Strategic Approaches to Intellectual Property

Patents and Blockchain Innovation

There are pros and cons between patenting and not patenting.

US Constitution gives inventor's exclusive rights to their discoveries to promote progress. But obtaining patents is expensive and can be speculative. Software innovation changes fast. A brilliant invention might soon be obsolete.

There is a more communal approach. The community would contribute to a database of filed patent applications. Anyone can check to see what's been published in a given field to avoid directing resources at the same subject matter. The US Patent and Trademark Office waits 18 months to publish applications. Companies could join within the community to share applications much sooner. Contributors might lose some strategic advantage, but the overall ecosystem could benefit by not duplicating efforts.

***Patent pools** are a mechanism for sharing issued patents to advance the overall industry. Individuals can choose to dedicate their patents to the public. Companies can assign patents to a trusted entity with a policy of non-enforcement. Patent pools can provide competitive benefits, and reduce transaction costs, sometimes clearing blocking patents from the market. Companies can cut their litigation costs.*

Blockchain essential patents are foundational. Any blockchain company would infringe them.
What if Satoshi Nakamoto had filed for and been issued a patent for the basic concept of Bitcoin, and thus the blockchain? It would be broad enough to encompass pretty much any application in the various blockchain business models, stifling innovation.

We could set up a pool of essential blockchain patents with volunteers managing the process.
The entity could function like the RPX Corporation. Members of the company pay dues, the company then buys patents or patent portfolios making them royalty free for members. Guidelines would define what makes a patent essential in the blockchain space. The evaluation would determine who required a license to the same patent. Stakeholders could receive value for participating in the evaluation process with credits on their yearly dues. The amount wouldn't depend on whether a patent is a essential or not. So an evaluator wouldn't feel pressure to inflate a patent's potential. Incentives could also go to individuals who volunteer to submit their patents to the essential patent blockchain. An open process could give companies a valuable view of the competitive landscape. There are drawbacks when individual companies invest in invention but received no compensation.

The proposed essential blockchain patent pool would use the best practices from earlier patent pools. Owners of patents deemed essential would be paid fairly.
It seems logical to use innovative technology to advance our technology law. **Using a blockchain for patent pools help streamline licensing, negotiation, and enforcement. Automated review systems become more feasible. High-fidelity tracking of changes is built-in, and it provides a testing bed for non-blockchain industries to move their pools to a blockchain system.**
But participation is crucial to ensure success of the blockchain essential patent pool. Voluntary communal coordination can also take place off blockchain. Individual companies don't have to share intellectual property, but community members could provide incentives for sharing. Companies could follow policies protecting some of their core intellectual property without being selfish. This approach would start with education. Industry leaders could agree upon a framework of suggested policies to share throughout the industry. Companies could be encouraged to publish open source blocking patents to the community. So blockchain-based technologies, and non-competing businesses wouldn't be blocked. Narrower patents confined to a vertical space will still protect the company's interests.

Payments, Attribution, and Licensing

Blockchain could transform the management of intellectual property rights from attributions and payments, to licensing and the management of rights. Collecting royalties could be fast and transparent on the blockchain.

Imagine royalty payments using cryptocurrencies.
Those could happen in minutes or seconds, whenever people downloaded a song or used it in their commercial. Or played it on the radio, or streamed it on Spotify,or bought ads around the music video on YouTube. ***Smart contracts*** *could track these different uses of a song and meter out royalties to the artists and to other stakeholders, all without human agents. That's the future on royalty payments on the blockchain.*

A distributed database built on blockchain for the creative industries would help artists register and protect their rights. Copyright is automatic upon creation of a work.
But the current registration process can be costly and involve multiple jurisdictions.
Blockchain platforms make global registration easier. An artist registers a work by uploading a digital file. The platform generates a hash of that file. A hash is a unique alphanumerical digest of the content. It serves as an identifier, like a digital fingerprint. It could be used for money like bitcoin. Or it could be used in this case for a song or a piece of art. **The creator secures attribution and timestamps possession of a file. That could be critical in a dispute over authorship.**

This registry would be available to anyone anywhere and scalable to billion of creative works. It would help creators get paid and help audiences fund the content that they wanted to consume. Streaming content would really mean streaming payments to artists.
Intermediaries could focus on helping audiences discover creative works instead of dealing with paperwork.
This distributive database would also help creators license their works with ease.
Digital certificates registered on a blockchain could store data on the rights status of a work, including conditions for use and for re-use. This data could unlock new revenue streams for creators.

Ease of licensing is important in the world of digital design.

Distributed Ownership

The blockchain could automate resale royalties and event ticketing. It could transform how organizations monetize fan data and create a more inclusive model for rights data.
The technology could even help creators to find new sources of capital and new models of distributed ownership. The blockchain makes decentralized collaboration possible for groups on a large scale.
One crucial feature of blockchain is the ability to align the incentives of people who don't know or even trust each other.

Backfeed is the name of an initiative launched to encourage massive open-source collaboration among a network of peers. It operates free of centralized control. Peers can use Back feed to evaluate contributions to a group project. Individual contributors receive rewards according to the perceived value of their work. It's a new form of commons-based peer production on the blockchain. Backfeed uses cryptographic consensus to solve the challenges of large-scale cooperation, but it keeps the benefits of commons style governance.

All-new forms of distributed autonomous art could be born on the blockchain.

> *The Plantoid Project which is also based on decentralized collaboration, but with a twist.*
> *Plantoid governance structure runs on the Ethereum blockchain. De Filippi called the Plantoid an artistic representation of a blockchain based life form. Its real-world body is a mechanical sculpture of a plant connected to the internet. It's Operating System is a smart contract. The Plantoid collects Bitcoin donations and responds with some form of appreciation. It might play a song, display a light show or perform a mechanical dance. It is actually fundraising for other projects.*
> *The smart contract has a targeted amount of Bitcoin to reach. When it reaches that amount, it issues a request for proposals for creating the next generation of Plantoid. Donors vote on the various proposals and Plantoid hires the artist whose submission receives the most votes to create an offspring. The Plantoid is a self-propagating artwork acting as an artist, art dealer, and agent. It achieves its own financial autonomy. It's the first instance of distributed autonomous art. This opens up a new set of possibilities for funding, commissioning, and making money from works of art.*