2234 Piedmont Avenue, Berkeley, CA 94720-2322 Phone: 510-642-3067 Fax: 510-643-6617
brie@socrates.berkeley.edu http://brie.berkeley.edu/BRIE/

BERKELEY ROUNDTABLE ON THE INTERNATIONAL ECONOMY (BRIE)
UNIVERSITY OF CALIFORNIA, BERKELEY

BRIE Working Paper 2016-1

Juri Mattila

THE BLOCKCHAIN PHENOMENON

The Disruptive Potential of Distributed Consensus Architectures

Juri Mattila is a Researcher at the Research Institute of the Finnish Economy (ETLA).

This paper has been published simultaneously as an ETLA working paper.

Table of Contents

1 INTRODUCTION

In November 2008, a mysterious white paper appeared on the Internet in all quietness. Written under the pseudonym *Satoshi Nakamoto*, the paper described a new method for creating a fully distributed digital currency system by cryptographically chaining blocks of data together. For many years, the technology behind that system went largely unnoticed by the general public. Today, however, seven and a half years later, that innovation is heralded as the next paradigm shift in digital networks, opening doors to an uncharted cyberspace of disintermediated trust and distributed consensus platforms.

While a lot of hype has been generated around blockchain technology, there are also those who have taken a more skeptical view on the phenomenon. At one extreme end of the spectrum there are those who say that blockchain technology will render national governments and their currencies obsolete, bringing about a new era of libertarian freedom and empowerment. At the other extreme people are predicting the complete self-destruction of the technology as a consequence of its own infeasibility.

There also seem to be notable differences in what people perceive blockchain technology to be in the first place. While Bitcoin puritans would only see the term explicitly used in reference to the infamous cryptocurrency itself, some would prefer to never even think about Bitcoin when discussing blockchain technology. Others find the whole division absurd, pointing out that blockchain is nothing more than a data structure and that such broad use of the term misses its mark entirely.

Whoever is right, one thing is quite clear: the terminology around the whole phenomenon is still heavily in flux. Caught in the middle of it all, it can be difficult to form a clear picture on blockchain technology and the phenomenon that surrounds it. As a result of all the hype and excitement, the development of the blockchain ecosystem is often perceived to progress so rapidly that in order to keep up, there is often a tendency to try to dive in too deep too quickly. Understandably, the big picture can remain blurry as a result.

This report was written with the simple goal of providing the reader with a more comprehensive understanding on what blockchain technology is, what its possibilities and limitations are, and what its potential larger societal implications may be. It aims to provide the reader with a holistic understanding of the key concepts and basic principles, thus equipping them with the tools and the framework to understand the ongoing discussion, to critically evaluate different viewpoints, and to delve deeper in a constructed manner.

In order to keep the descriptions as simple as possible, some technical details have been simplified to make way for a clearer big picture. In places, some technical commentaries have been included in the footnotes but those primarily looking for a detailed technical description will most likely be more satisfied with other sources of information.

The technical information presented in this report is mostly based on unstructured discussions with representatives from companies such as IBM, BitPay, Blockstream, Vaultoro, Colu and Bitreserve in Barcelona in October 2015; with representatives from Google, 21 Inc and Stellar in San Francisco in February 2016; with representatives from Eris Industries and Ascribe in Berlin in March 2016; and with representatives from Prasos Oy (Bittiraha.fi, Coinmotion, Denarium) and Robin Hood Minor Asset Management Cooperative in Finland in March-April 2016.

This paper has been drafted as a part of the BRIE-ETLA research collaboration of 2015-2018 and it has also been published simultaneously as an ETLA working paper. The author would like to thank emeritus professor John Zysman from the University of California at Berkeley, professor Martin Kenney from the University of California at Davis, BRIE research fellow Jonathan Murray, Timo Seppälä from the Research Institute of the Finnish Economy and Aalto University for their insightful discussions and commentaries while writing this report. The author would also like to express his gratitude to all the participants of the BRIE-ETLA roundtable discussions at the Claremont Hotel in Berkeley in February 2016.

2 UNDERSTANDING THE TECHNOLOGY

2.1 Why all the fuss?

In digital networks, data is usually transmitted by copying it from one place to another. One of the key problems in this respect is *how to verify that the information received from the network is authentic and up-to-date.* While this is not a particularly difficult problem to solve in itself, so far all the solutions have required placing trust in someone. In many cases, taking the word of a trusted authority for the authenticity of data is perfectly fine, but in some cases it is really not. Moreover, even when it is fine, constantly having to resort to an intermediary is often expensive, and it would be a lot cheaper if we simply did not have to.

The reason why blockchain technology is considered so disruptive is that it has the ability to solve this problem of authenticity without the inclusion of any trusted intermediaries. It allows anyone to verify the authenticity of data independently, without having to take someone else's word for it, irrespective of whom or where that data came from in the network.

To understand the full scope of the potential implications of this change, one only has to consider the fact that most of us rely on trusted intermediators in our daily lives most every day, in one form or another. Whether it is locking your house with keys made by the local locksmith, trusting an online vendor with your personal information, or even having faith in that the products you purchase have been tested for safety, we all depend on trusted intermediators in ways that we don't necessarily consider problematic, but would gladly get rid of in a heartbeat if provided with the opportunity.

Overall, blockchain technology is disrupting society in two fronts. Firstly, it is providing disintermediated, censorship-resistant and tamper-proof digital platforms of distributed trust, open for all to freely innovate and to transact on. In doing so, blockchain technology introduces new elements into the discussion on the platform economy and the related key questions: how is value created around platforms, who captures the value and who owns the platforms themselves.[1]

Secondly, for enterprise- and industry-level systems, it is providing efficiency gains on top of existing structures by removing the constant need for actively intermediated data-synchronization and concurrency control.

Due to this dual effect, blockchain technology has the potential to impact all sectors and layers of society, in a multitude of combined ways. Whether it is with completely novel solutions to interacting over the internet or with increased efficiencies in pre-existing industrial systems, there are benefits to reap in all playing fields — and those who neglect to do so may just end up finding themselves at a disadvantage.

[1] Kenney–Zysman 2016.

2.2 Blockchain terminology

The definition of the term *blockchain* is far from clear.[2] The word *blockchain* itself most likely traces back to Satoshi Nakamoto's original Bitcoin white paper from 2008[3]. While there is no specific mention of the word blockchain in the paper, it describes a technology component underlying the cryptocurrency as a series of data *blocks* that are cryptographically *chained* together. While most of the components described in the paper have existed since the 80's and the 90's, the author's contribution was to apply them in an innovative way, combining them into one functional cryptocurrency system.

Using this etymology, strictly speaking blockchain is nothing more than a mere data structure with distributed multiversion concurrency control. When the term first became popular, however, there was only one practical application of this data structure in existence: the Bitcoin cryptocurrency. Due to the lack of any pre-existing architecture, Bitcoin, by necessity, constituted the entire technology stack of the distributed consensus architecture.

Later on, companies such as Ethereum, Eris and Filament started looking beyond Bitcoin and focusing specifically on individual layers of the technology stack (see table 1). As a consequence, the stack quickly became fragmented along with the nomenclature, and the terminology of blockchain was extended to describe a multitude of different structures at a variety of different levels of the stack.

Table 1. A coarse depiction of the "blockchain technology stack"[4]

Layer	**Example of a blockchain-related product/service situated in the layer**
Application layer	Ujo Music
Platform layer	Eris Industries' smart contract application platform
Processing layer	Ethereum virtual machine
Data/Protocol layer	The Bitcoin blockchain
Network layer	Filament Tap
Hardware layer	BitFury mining chips

[2] Systems with somewhat similar cryptographic functions are sometimes used for other purposes that are not usually associated with blockchain technology. Conversely, not all distributed databases necessarily make use of the kinds of cryptographic functions that usually are associated with blockchains.

[3] Nakamoto 2008.

[4] Pon 2016.

As the phenomenon of distributed consensus architectures progressed, the use of the term blockchain in reference to it on a societal level also grew more popular. Expressions such as *the blockchain economy* and *blockchain revolution* became more commonplace. Much like with *cloud* or *big data* in recent years, the term *blockchain* is now quickly becoming a vacuous buzzword, and it is specifically due to this lack of clear terminology that the blockchain phenomenon overall can be very confusing to try to understand.

Due to the lack of a more descriptive established nomenclature at this time[5], this report uses the term *blockchain technology* somewhat broadly, mostly in reference to the entire technology stack of distributed consensus architectures.

2.3 The carrot, the stick, and the database democracy

While the terminology around the blockchain phenomenon is ambiguous at best, the core concept behind the technology itself is, in fact, quite simple. When a database needs to be modified by multiple parties at the same time in an overlapping manner, either their modifications have to be somehow consolidated together, or multiple differently modified versions of the same database will emerge. For some databases, such as software code repositories, multiple versions pose no problems, as long as the different versions are tracked accordingly. Other databases, such as financial ledgers, however, rely on maintaining only one absolute version of their modification history and content.

The traditional approach to ensure that only one modification history persists has been to introduce a central authority who exercises concurrency control over the entire database. While this method solves the problem of overlapping concurrent modifications, it introduces a whole new set of derivative problems in the process. For example, a central authority introduces costs and has to be trusted to behave honestly.

Blockchain technology enables a more effective way to solve the concurrency problem in a completely distributed manner, without the caveats of a centralized solution: Instead of having a central authority that maintains a database and guards its authenticity, a copy of the entire database is distributed to an open cloud for every willing participant to independently maintain. The copyholders then follow a predetermined set of database management rules and compare their versions together through a continuous process of voting[6]. The version

[5] The term *distributed ledger* has also been suggested by some to clarify the ambiguous blockchain terminology. While such a term could be useful in some ways, it presupposes an emphasis on tracking assets in contrast to tracking processes. Furthermore, the proposed term does not properly acknowledge the presence of a distributed consensus mechanism which — many would argue — is at least as significant a part of the blockchain phenomenon as the blockchain data structure itself.

[6] In technical vernacular, the voting process is traditionally called *mining* and the participants or *nodes* involved are referred to as *miners*. This is due to the fact that in the first blockchain application, the Bitcoin cryptocurrency, the output speed at which the voting rewards increase the Bitcoin money supply was designed to mimic the speed at which the mining of gold increases the global gold supply.

that gets the most votes from the network is accepted as authentic, and the process repeats indefinitely.

To avoid mendacity amongst the participants, a clever incentive structure is woven into the voting process: Voting with the majority — that is, for the version of the database that in time ends up being accepted by the network as authentic — is rewarded, while voting against the majority rule is punished. This produces a game-theoretical equilibrium where all the participants are best off trying to anticipate each other's choices and try to vote for the version of the database that will eventually be accepted as authentic.[7]

In other words, instead of a central authority keeping everything in sync and dictating the modification history of the database, with blockchain technology every participant gets a say in what they think the true course of events has been. It is a new way of organizing and managing databases in a leaderless democracy of devices, incentivized to work together for one shared consensus view.

2.4 Permissioned and permissionless blockchain architectures

Looking at the entire technology stack of distributed consensus architectures, each layer in the stack can be constructed in multiple different ways, some of which have mutually exclusive properties. Therefore, it is impossible to give an exhaustive answer to what the characteristics of blockchain technology are, in such a meaning of the term. It is possible, however, to characterize what kinds of different blockchain architectures there can be.

A rudimentary division that is often made between different kinds of blockchains is that of *permissioned* and *permissionless* blockchains. So far, this report has mainly described the characteristics of permissionless blockchains. Such blockchains are completely open access to everyone and no permission is required from any authority to become a participant in the network. Participants are unknown to each other and trust emerges from game-theoretical incentives.

The idea behind permissioned ledgers is no more complicated: If all the participants in the network are known and can be trusted to vote honestly, there is no need to introduce the artificial incentives to ensure that co-operation will take place. To facilitate the possibility of a negative outcome, these incentive structures often involve spending physical resources, such as computing power which translates into wasted electricity. On an aggregate level, this expenditure can quickly become quite significant. Thus, by only permitting trusted members to participate in the voting process, the operation of the network can be made faster, more flexible and most importantly, much more efficient — but at the cost of reduced security, immutability and censorship-resistance.

[7] Several different voting systems, or *consensus mechanisms*, have been developed, each one of them with its own unique features and intricacies. For a more detailed comparison, see appendix 1.

More sophisticated consensus algorithms are constantly being developed, but at least for the time being, one of the intrinsic properties of blockchain applications is that in their design, there are always inevitable trade-offs to make (see table 2).

Table 2. Trade-offs between different types of blockchain architectures (simplified)

	Permissioned	Permissionless
Fast	☑	□
Energy-efficient	☑	□
Easy to scale	☑	□
Censorship-resistant	□	☑
Tamper-proof	□	☑

2.5 Generic and specific blockchain architectures

Another dimension by which to characterize blockchain architectures is whether they are optimized for a specific task, such as tracking assets and transferring value, or a more general purpose, such as storing algorithmic code and running customized logical processes. Roughly, the division is somewhat analogous to the difference between a Swiss army knife and a specific special purpose tool. The first is more versatile and allows more functions, but if all that is needed is a simple function to be performed well, then a special purpose design may just be the sensible choice.

Blockchain platforms designed for a general purpose, such as Ethereum and Eris, allow users to write their own programs to be stored on the blockchain and automatically executed in a distributed manner. They serve as programmable consensus engines, ready to be utilized for whatever purpose the users wish to bend them. Special purpose designs, however, are much more limited in this respect and usually do not allow users to deviate very far from their originally designed uses (see table 3).

Table 3. Examples of different blockchain architectures[8]

	Permissionless	Permissioned
General purpose (Optimized for logic)	Ethereum	Eris
Special purpose (Optimized for assets)	Bitcoin	Hyperledger

2.6 The challenges of the blockchain ecosystem

When projecting the future growth of the blockchain ecosystem, it is often argued that the technical capabilities of blockchain-based distributed platforms are in many ways superior in comparison to more conventional platform solutions. When it comes to speculating on the technology standards of the future, however, the essential question is that of a critical mass. In order to become a thriving technology, technical superiority alone does not suffice. The adequate presence of three factors is also required in the blockchain ecosphere: demand, competition, and know-how.

According to blockchain technology developers, there are roughly a thousand companies in the world focusing on blockchain-related innovations at the moment. Only a small fraction of these companies are working on actual blockchain technology development. At this point, it is still uncertain whether the knowledge and the understanding on this technology will spread enough to attract sufficient numbers of customers, entrepreneurs and developers to reach the critical mass of a stable mainstream ecosystem. Furthermore, many other factors, such as changes in regulation and disruptive developments in competing technologies can affect the attraction in unpredictable ways.

In terms of individual distributed platforms, it is important to bear in mind that, like the ecosystem, they too live and die by network effects. In has been pointed out in platform discussion that fostering network effects is a delicate balancing act, and building successful platforms is difficult at the best of times.[9] Therefore, it is unclear at this point whether network effects can be sufficiently nurtured in distributed platforms in general, especially in an aggressive competition environment where centralized platform companies are actively fostering their own network effects through constant, carefully thought out strategic decision-making.

[8] Adopted from Eris Industries 2016.

[9] Hagiu 2014.

3 APPLICATIONS AND USE CASES

3.1 Financial instruments, asset registries and marketplaces

As it has already been established, blockchain technology can be used to create immutable and censorship-resistant distributed records of any content. One very useful way to apply such a technology is for records of ownership. These records can contain ownership information about any asset to which a unique identifier of some kind can be issued, regardless of whether the asset itself is of digital or physical nature.

Blockchain technology allows records of ownership to be constructed in such a way that anyone can make additions to the database by adhering to a predefined ruleset. This allows the record of ownership to be extended into a payment transaction network for currency, or a marketplace for any other financial asset for that matter.

Blockchain-based value transfer and storage systems have certain technical benefits compared to conventional systems. For private individuals, they can bring increased security, more privacy and better control over their personal financial assets.[10] To businesses, blockchain technology enables lower payment processing fees, accepting payments from anywhere in the world, and reduced or eradicated risk of chargeback fraud.

Blockchain technology can, however, also improve the efficiency of the existing structures of value transfer between payment processors, such as banks and credit card companies. One way such improvements can come about is the reduction of the settlement time between banks from several banking days down to a number of minutes, or even seconds.

Case: Coloured Coins with Colu

Colu is a digital asset issuance and management service built on top of the Bitcoin blockchain. The service allows the issuance of digital assets through a process called *colouring.* In this process, a certain small unit of bitcoin is marked and used as a token of ownership for the issued asset. By then sending the small token through the Bitcoin network, the ownership of the attached asset itself can also be verifiably and securely transferred, as easily as sending an e-mail.

[10] It should be pointed out that these benefits only apply if the individual is behaving responsibly with their digital assets. Over the past few years, there have been many cases presented in the media where bitcoins or some other cryptocurrency has been stolen from a user's account. While cryptocurrency payments would be extremely difficult to falsify and the blockchain system in itself is very rigorous, unsafe passwords can still be cracked, just as with any system. Just as with physical cash, where the anti-counterfeit security features on bank notes cannot protect the users against their money not being locked up properly, the tamper-proof nature of blockchains cannot help those using weak passwords to secure their accounts.

Case: Stellar & Oradian – Microfinance integration in Nigeria

The multitude of microfinance institutions in Nigeria is immense, with the number of individual branch offices extending to tens of thousands. Formerly, these branch offices have lacked any practical means to make transactions between each other. Therefore, the vast rural population of Nigerians not eligible for conventional banking services have had to rely on physical deliveries of cash to send money from one branch office to another. Needless to say, speed, cost and security pose massive problems for those needing to engage in such transactions.

Stellar is an open-source platform that allows users to create financial products and services amongst themselves using blockchain architecture. Allowing 300,000 transactions for the cost of a single penny, Stellar has taken on the challenge of providing integrated microfinance services all across Nigeria. Since February 2016, Stellar has been running a nation-wide test network in co-operation with the microfinancing software provider Oradian, covering a total of 200 branch offices and reaching 300,000 end users. Over 90 % of the current customers are female, implying that the full-scale integration of microfinance services could be a significant factor in the economic empowerment of women in the developing world.

Case: OpenBazaar – A distributed free marketplace

OpenBazaar is a blockchain-based, fully distributed e-commerce platform that enables totally free transacting between any willing parties directly amongst themselves. Since the users of OpenBazaar produce the trading platform amongst themselves as a distributed network without any intemediators, there are no transaction fees or trading restrictions of any kind.

In other words, no party has the power to censor the buying and selling that takes place on the network, or to freeze the associated payments, if the transactions are settled in cryptocurrency. The transacting parties are free to disclose as much or as little about themselves to each other as they want, and they are free to transact directly without any outsider involvement whatsoever. If so desired and agreed, however, the parties can hire any moderator of their liking to oversee their trade and to resolve any potential disputes that may arise. In such a case, the buyer, the seller and the moderator all have their own cryptographic key, two of which are required to execute the contract.

3.2 Nanopayments

Another interesting prospect of blockchain-based value transfer systems is the possibility of making very small transactions, potentially as tiny as a fraction of a penny, economically viable. In conventional payment transaction systems, there are fixed costs and technological limits involved which so far have rendered such transactions more or less unfeasible on a large scale.

Nanopayments can enable completely new business models for online content creators where customers could be charged for news articles, videos and other such content on a direct pay-per-view basis. This could have a notable impact on the short-sighted content creation logic currently exploited by so many online media houses. Instead of creating click-baiting news headlines just to attract more views for the ad banners on the website, companies could be more accurately rewarded for creating insightful and meaningful content that the readers truly enjoy, irrespective of how many ad banners are shown and how many clicks the website generates.

Due to the versatile programmability of cryptocurrencies, other less intuitive use cases can also be presented for blockchain-based nanopayments. For example, tiny, automated transactions could be utilized as an e-mail spam filter that would be very difficult to circumvent. By setting a nano-scale price tag on sending an e-mail message, the cost would be insignificantly small to any normal use of e-mail, but it would quickly grow to prohibitive proportions when attempting to send millions of spam e-mails.

Some have argued that the whole concept of micropayments is inherently flawed because the cognitive transaction costs of operating in an environment requiring constant micropayments would be too high. The benefit of using blockchain technology in this respect is that it allows the payments to be automated to a much higher degree than previously has been possible, therefore allowing lower cognitive transaction costs and more convenient usability.

Case: ChangeTip

ChangeTip is a cryptocurrency-based micropayments platform which allows attaching real monetary value to online social interaction. The idea is that instead of simply pressing a like-button to express appreciation towards a blog post, for example, ChangeTip allows people to send tiny tips on any social media service in real time, just as easily as pressing a like-button. By significantly lowering the threshold of rewarding content and small services, such as providing a quick answer to someone's question on the social media, small tips of individual cents could become as common and casual as "likes". In such a scenario, the tips received from active social media participation could amount to a free beverage at the end of the day, for example, or even a notable part of the daily income for someone more popular.

The concept of ChangeTip has raised some criticism as to whether people actually want to slap price tags on their social interaction. While this criticism may well be founded, the fundamental idea behind the service could have wider implications on how we perceive and valuate the digital economy. Currently, there is a lot of work and content creation happening online which doesn't show up in any financial metrics of the economy at all. Largely, this is due to the decoupled nature of digital goods/services from their respective cash flows, but one factor in the problem has been that there is no objective measure for the value of gratuitous social media interaction. Blockchain-based micro- and nanopayments could, in theory, provide a market-driven solution to such valuation problems, thus providing improved metrics and a more detailed picture of the new forms of economic activity in the 21st century.

3.3 Identity management and online reputation

The immutable and distributed nature of blockchain databases can also be utilized for identification and reputation management. The common problem with the digital identification methods currently available is that they mostly rely on a trusted intermediator to verify the authenticity of an identity. This introduces service fees and gives the intermediator all the power to decide which service providers are allowed to make use of the verified identity.

Moreover, in Finland, for example, digital identification services have mainly become an established domain of banks and other financial institutions. As such, they have legal requirements, as well as their own economic interests, to know their customers to a much higher degree than would be required to simply establish a verified identity. Consequently, anyone willing to identify themselves online, is forced to give out much more information about their sources of income and financial situation than is actually necessary.

Blockchain technology brings improvements to the contemporary digital identity services in two fronts. Firstly, it removes the need to go through a trusted third party, thus eliminating the service fees involved. It also nullifies any artificial requirements to disclose private information about oneself in contexts where it is not relevant to the task at hand.

Secondly, blockchain technology makes digital identities more ubiquitous in that they can be freely integrated to any service where the identity holder and the counterparty together wish to do so. This makes online reputation much more pervasive and meaningful, potentially leading to a digital environment where complete strangers are significantly easier to trust due to their documented reputation.

Case: Bitnation

Bitnation calls itself a “governance 2.0” service. Powered by blockchain technology, the organization seeks to provide all the same services as traditional governments but in a globally distributed manner. In addition to validated identities, Bitnation currently offers notarization, dispute settlement, and some other related services.

Since December 2015, Bitnation has been collaborating with the Estonian government to offer public notary services to Estonian e-Residents. By signing in with their electronic IDs, Estonian e-Residents from all over the world can now officially notarize birth certificates, marriage arrangements, testaments, business contracts, land titles, or any other such documents through Bitnation’s service.

During the recent European refugee crisis, Bitnation has also been running a refugee emergency response program, providing refugees with authenticated identification documents that can help in reuniting families, debit cards that are directly linked to accounts of donated cryptocurrency, and other such immediate first-hand services.

3.4 Supply chain records and product-centric data

When customers are looking to buy products, they are currently very limited in their ability to evaluate the origins of the materials used or the ethical aspects of how products have been manufactured. What's more, even companies themselves cannot always keep track of the legitimacy of their complex supplier networks. Blockchain technology has the potential to bring massive improvements to this by providing companies and consumers with access into detailed and immutable supply chain records, on the level of individual products.

As a practical example, a customer wanting to purchase a frozen meal of fish curry could scan a QR code on the item to see where the ingredients came from, how much was paid to each producer and whether or not the product has been maintained within the proper sub-zero temperature range throughout its logistical journey. Not only would this significantly enhance product safety, but it would also empower consumers to vote with their wallets much more efficiently to weed out bad actors.

Another twist of essentially the same idea could be applied in industry. Instead of all the companies in the supply chain maintaining their own individual production models and local copies of the product data, all that information could be stored in a distributed blockchain database and tied to the corresponding products and components. This way, all the different file versions could not fall out of sync and become obsolete, and all the product data would always be verifiable as authentic. As a result, losses resulting from adhering to incorrect production models could significantly be reduced leading to more efficient production.

Case: Everledger – A distributed diamond certification database

Everledger is a company that specializes in tracking diamonds using laser-inscribed serial numbers, digital thumbprints of attributes, and a distributed blockchain database. Thanks to providing an effective method of keeping track of the origins, the movements, the ownership trail, as well as any other events and news articles involving certain specific diamonds, a buyer or an authority coming across a precious stone can easily verify whether it has been involved in a theft, a fraud or any other kind of unethical activity.

Records like Everledger could also be utilized in other complementary ways. They could act as information repositories for various kinds of smart contracts that involve transporting physical goods.
This, in turn, could bring significant clarity into the value added tax system in Europe, for example, where online vendors are required to charge the VAT according to each buyer's country of residence individually.

3.5 Smart contracts

The idea of smart contracts is that by formulating contractual arrangements between parties into computer code format and storing them into a blockchain, contracts can be made tamper-proof, self-executing and automatically enforceable. By reducing the need for routine human intervention, the entire contractual process can thus be made less risky and more cost-efficient.

In order to convert a conventional paper contract into a smart contract form, it must be possible to represent the arrangement as a logical flow chart of "*if X, then Y, else Z*" types of dependencies. Contracts, however, often involve a degree of ambiguity as to whether a specified condition has been adequately met or not. While there are various solutions that have been proposed to this problem (such as utilizing distributed prediction markets or multi-signature encryption keys), the truly interesting question is whether entirely new automated contractual techniques will emerge which, at least in some cases, allow such ambiguities to be averted completely.

The possible use cases of smart contracts are virtually endless, extending from e-commerce to autonomous machine-to-machine transactions, and from pre-contracted budgets to automated access control. One example would be an automated lease contract on a vehicle that would revoke the user access to the asset if the proper payments have not been made accordingly.

Case: Ujo Music – A decentralized music platform

The settling times in modern day banking are sometimes considered excessively slow, often taking several banking days to clear. In the music industry, however, the time that artists have to wait for royalties for their work is usually measured in years. Ujo Music is a service which uses the blockchain-based smart contracts platform Ethereum to bring music licensing to the 21st century. Ujo's service allows artists to record their work into a blockchain as a smart contract which specifies the shares that each contributor gets of the revenue. Once a person downloads the song and pays for it in crypto-currency, the payment is instantly channelled to all the contributors through the smart contract in real time.

Ujo Music also introduces new capabilities that the current archaic licensing framework of the music industry does not allow. For example, through Ujo Music, an artist wishing to remix an existing song can download just the isolated vocal track by agreeing to the contractual terms specified by the singer in the smart contract. For example, the singer might have stipulated that the vocals are available for any non-commercial use for 50 euros, and for any commercial use for 25 % of the remixed song's total revenue. Anyone agreeing to the predefined terms of the smart contract can immediately acquire the pieces they need to start remixing, without having to contact record labels, studios or even the artists themselves. An acceptance of terms of the smart contract will suffice, and the royalties from any revenue that the derivative work generates will be channelled to the original singer in real time, just like with the original work itself.

3.6 Internet of Things

There are many proposed platforms and standards in existence today that could function as a basis of a ubiquitous network of smart systems, commonly referred to as the 'Internet of Things'. Most of these platforms and standards, however, are based on a centralized architecture, to one degree or another. While centralized systems are often cheaper and easier to construct, they might not be what is best for the Internet of Things as a whole.[11]

Understandably, companies are usually reluctant to submit into operating within technical frameworks that are controlled by other companies. In general, this makes a lot of sense, of course, as getting locked into someone else's platform usually means becoming the underdog in terms of value capture potential. Therefore, companies would rather create their own company-specific or consortium-based systems.[12]

If the architecture of the entire Internet of Things consisted of countless such company- or consortium-level platforms, the interoperability between all the different platforms bubbling into and out of existence would present a huge challenge to seamless large-scale functionality. Conversely, if a small number of platforms managed to foster enough network effects to grow into universal IoT platforms, such centralized solutions could easily be turned into vertical silos, or so-called walled gardens. In other words, the company in control of the platform could by design purposefully reduce interoperability with other platforms in order to enforce a stronger customer lock-in to its own domain of products and services.[13]

So, one could argue that building network-of-systems-level IoT platforms with strong network effects is difficult because of there are inherently conflicting interests between the platform participants and the platform providers. Blockchain technology could provide a way to circumvent this problem by offering a neutral territory where all participants can operate on a shared platform, on completely equal footing. Instead of the platform provider being the dominant player to the power of whom all others must submit, blockchain technology could enable all the participants to produce an IoT platform together in a distributed manner, without having to trust each other in almost any capacity.

[11] Mattila–Seppälä 2015.
[12] Seppälä–Mattila 2016.
[13] Filament 2015.

Case: The 21 Bitcoin Computer

21 Inc is a company specializing in embedded computer hardware with native support for cryptocurrency transactions. After raising $121 million of venture capital last year, 21 Inc has launched a developer version of the 21 Bitcoin Computer – a portable cryptocurrency micropayment server with an integrated mining chip. The device has native protocol support for various cryptocurrency-related functions, so that by simply adding one line of code into its computer program, the device can, for example, be told to execute a cryptocurrency payment, or to wait until a payment is made to its account before continuing its program.

The company's vision is to eventually incorporate a mining chip into every digital device, so that cryptocurrency mining capacity would ultimately constitute one fundamental system resource in computers alongside the CPU performance, amount of bandwidth, memory capacity, and hard disk space. With each device's stock of cryptocurrency constantly replenishing through the process of embedded mining, digital value transactions could be conveniently automated between devices by writing them directly into the computer program of virtually any device.

In essence, 21 Inc's concept would allow for IoT devices to transact directly amongst themselves, without the need for any centralized background architecture. While enabling cost-savings and increased network robustness, the 21 Bitcoin Computer could in time also allow devices to autonomously exchange other resources than mere data, such as computing power, bandwidth, storage space, or even electricity, thus bringing us one step closer to the feasibility of IoT.

3.7 Voting systems

Online voting systems can be problematic to build because of the complex requirements of neutrality in such systems. To ensure a fair election, online voting systems must remain anonymous yet auditable, as well as tamper-proof but unintermediated. Blockchain technology is very appealing in this regard because from a technical standpoint, it has the rare ability to tick all the right boxes.

There are many possible ways to create a blockchain-based voting system but the simplest description is that, in essence, they work much the same way as a cryptocurrency. The main difference here is that instead of transferring tokens of monetary value between accounts, the tokens transferred in the network are used to describe individual votes transferred into ballots.

Due to the fact that blockchains can be designed to be public yet anonymous, anyone can easily verify the voting outcome and also check that their own vote has been taken into account accordingly, while still maintaining ballot secrecy. Blockchain technology can therefore help to reduce corruption in political systems and act as a safeguard against rigged elections.

3.8 Decentralized autonomous organizations

To give an idea of the wider unexplored potential of blockchain technology, one of the more exotic ideas is to create so-called *decentralized autonomous organizations*, or DAOs. The argument is that by combining cryptocurrency with self-executing smart contracts, it is possible to create a network of automated nodes that operate together as a system without any external human guidance, according to an incorruptible protocol specified in computer code and enforced automatically on the blockchain.

One way to conceptualize decentralized autonomous organizations is to think of them as the opposite case of robotic systems (see table 4). In robotic systems, humans are used to organize machines operations while in decentralized autonomous organizations, machines are used to organize human operations.

Decentralized autonomous organizations could in time be assigned the role of many organizations in today's society. Especially in situations where the purpose of the organization is to provide goods and services to its owners, as is the case with co-operatives, decentralized autonomous organizations provide interesting future prospects.

Case: Neureal – A distributed artificial intelligence platform

Neureal is a project utilizing blockchain technology to create an open distributed platform for artificial intelligence algorithms. The idea is that the nodes of the network run various AI algorithms that make predictions on any desired input data from the outside world. Any willing participant is free to add their own node with their own AI algorithm into the network. The most accurate predictions are rewarded with cryptocurrency which over time leads to an evolutionary development towards more accurate powers of prediction. The nodes in the Neureal network can independently purchase predictions from each other to utilize as a part of their own analytics. This means that the nodes can autonomously arrange themselves into a hierarchical structure, greatly resembling the mechanics of a deep learning machine in this respect.

Currently, Neureal is still in a very early phase of its development. In time, however, such blockchain-based neural networks could theoretically lead to the commoditization of artificial intelligence algorithms entirely. In such a scenario, anyone would be able to participate in the algorithmic economy and to innovate as its fully empowered member.

It is well possible that nothing might ever come out of Neureal. More than anything, however, it is a good illustration of the fact that not all disruptions and use cases of blockchain technology have yet been charted, nor are they intuitively clear at the first thought.

Table 4. The relationship between different kinds of automated systems.[14]

	Humans on the edges	**Automation on the edges**
Humans in the center	Human organizations	Robotic systems
Automation in the center	Decentralized autonomous organizations (DAOs)	Fully automated systems and systems of systems

[14] Adopted from Buterin 2014.

4 IMPLICATIONS

4.1 Digital trust redefined

One of the fundamental disruptions that blockchain technology is causing is that it completely redefines how trust is perceived in a digital environment. In essence, blockchains have introduced a completely new type of digital trust which manifests itself in a fully distributed way without anyone having to trust any single member of the network. The only trust required is in that, on average, the participants of the network are behaving honestly — or more to the point, that the majority of the entire network is not colluding against the others in a coordinated manner.

By removing single points of failure where dishonesty would be detrimental to the integrity of information, blockchain technology has opened a door to a more democratized space of social and economic activity. As we transition from a cyberspace where trusting unknown counterparties is hard into a digital world where transacting with strangers is easy, we can expect to see new trends of more direct and decentralized economic activity in all frontiers.

4.2 The trend of disintermediation

In our modern society, the role of many intermediaries can be essentially reduced to one thing: facilitating trust between parties. In a digital environment, it is often difficult to trust that private individuals are who they say they are, and that they will do what they promise. Big companies, however, stand to lose more in goodwill damages than they stand to gain from breaching a contract with a customer. As this is more than can be said of unknown individuals online, companies have built businesses around intermediating trades by lending their trustworthiness to the cause – but for a price.[15]

By offering a technical solution for digital interaction where trusting counterparties is simply not necessary, blockchain technology can render intermediators, or at least their current functions, obsolete. As a consequence, the business mechanics and value creation logics of intermediation platforms may be in for a shock where trust, or the lack thereof, is not enough in itself to ensure customer lock-in anymore.

[15] Mattila–Seppälä 2016.

4.3 Democratization of the supply chain

Another effect potentially resulting from the digital trust and disintermediation trends is the reconfiguration of the balance of power in supply chain networks. Up until the present day, decisions relating to the supply chain of a product have mainly fallen within the domain of companies. Even if customers were able to have some idea of what kinds of raw materials and labour inputs went into the products, they would seldom have any visibility into the division of costs and profits in those supply chains — not to mention any decisive power over such matters.

Due to the increased visibility into supply chain networks enabled by blockchain technology, customers are able to demand much more detailed information about their products and services. With blockchain applications, consumers could even specify minimum and maximum prices that they are willing to pay for each ingredient and labour input individually and then scan for products that meet their specified criteria.

Alternatively, taking things one step further, consumers could even utilize smart contracts to customize the entire production process to match their own consumer preferences. In other words, instead of choosing a standard product from a vendor's catalogue, the consumer could transact with the producers and manufacturers directly. By doing so, the customer could arrange each step in the supply chain to their own liking, using specified raw materials and suppliers for a product produced exactly as the customer wants it. Smart contracts could even allow consumers to automate the optimization of all the parameters, so that if a more optimal contract for a certain production phase is offered, it is automatically accepted and incorporated into the chain of production.

4.4 A shift towards an automation economy

Self-executing smart contracts constitute a big part of the disruptive potential of blockchain technology. While they will undoubtedly reduce transaction costs between humans, their true disruptive potential lies with machine-to-human and machine-to-machine contracts. Combined with micro-payments, machine transactions could enable completely new kinds of business models. For example, autonomous distributed markets could help to allocate production resources much more efficiently between individual products and components on an automated, constantly adjusting *ad hoc* basis. Individual components could autonomously accumulate wealth in order to cover their own maintenance and recycling costs.[16]

[16] Mattila–Seppälä 2015.

4.5 Reconfiguration of regulatory capacity

The legal conventions of a given era often reflect what is technologically possible in that particular time period. As blockchain technology disrupts societal systems, it also reconfigures the regulatory capabilities that regulating authorities have in those systems.

For example, since it has not been previously possible to transfer value over the Internet without mediation from a trusted third party, these mediators have provided a natural choke point for financial regulation. By introducing direct legal requirements and obligations for payment processors, regulators have been able to govern the entire field of electronic value transactions indirectly. The same holds true in many other fields of society just alike. Wherever intermediators have been necessary to facilitate online interaction, regulation has often become shaped by this fact.

Due to its disintermediating effect, blockchain technology may well render some of the old regulatory strategies obsolete. However, it also introduces some novel technological abilities that can be useful for entirely new regulatory approaches. The increasing significance of computer code in governing economic behaviour in society means that the possibility of affecting behaviour by regulating computer code through standards, for example, is also increased.

Furthermore, other regulatory benefits can also be pointed out, such as increased transparency and automatization. For example, with the help of smart contracts, custom tariffs and taxes related to international trade could be automated to a much higher degree than today. By tapping into asset tracking databases, such as Everledger, the movement of goods into and out of the country could be automatically detected and used as an event trigger for automated tax payments and deductions.

The shift in regulatory capabilities towards a more technological centre of gravity may also have an impact on what kind of regulatory competence is required of legislators and other government officials in the future.

References

Buterin, Vitalik (2014) *DAOs, DACs, DAs and More: An Incomplete Terminology Guide.* <https://blog.ethereum.org/2014/05/06/daos-dacs-das-and-more-an-incomplete-terminology-guide/> Accessed 14th April 2016.

Eris Industries (2016) *What is a Blockchain?* <https://docs.erisindustries.com/explainers/blockchains/> Accessed 14th April 2016.

Filament (2015) *A Declaration of Device Independence.* <https://medium.com/@FilamentHQ/a-declaration-of-device-independence-b6f83e8b6441#.flo8gr95x> Accessed 14th April 2016.

Hagiu, Andrei (2014) *Strategic Decisions for Multisided Platforms.* MIT Sloan Management Review, Vol 55(2), pp 71–80.

Kenney, Martin –Zysman, John (2016) *The Rise of the Platform Economy.* Issues in Science and Technology 32(3), p. 61–69.

Mattila, Juri – Seppälä, Timo (2015) *Blockchains as a Path to a Network of Systems – An Emerging New Trend of the Digital Platforms in Industry and Society.* ETLA Reports 45. <http://www.etla.fi/julkaisut/blockchains-as-a-path-to-a-network-of-systems-an-emerging-new-trend-of-the-digital-platforms-in-industry-and-society/> Accessed 14th April 2016.

Mattila, Juri – Seppälä, Timo (2016b) *Digital Trust, Platforms, and Policy.* ETLA Brief 42. <http://www.etla.fi/julkaisut/digital-trust-platforms-and-policy/> Accessed 14th April 2016.

Nakamoto, Satoshi (2008) *Bitcoin: A Peer-to-Peer Electronic Cash System.* <https://bitcoin.org/bitcoin.pdf> Accessed 14th April 2016.

Pon, Bruce (2016) *Blockchain will usher in the era of decentralised computing.* <https://www.linkedin.com/pulse/blockchain-usher-era-decentralised-computing-bruce-pon> Accessed 14th April 2016.

Seppälä, Timo – Mattila, Juri (2016) *Ubiquitous Network of Systems.* BRIE Research Note 1/2016. <http://www.etla.fi/julkaisut/ubiquitous-network-of-systems/> Accessed 14th April 2016.

Appendix 1. Examples of consensus mechanisms.

Consensus mechanism	Scarce voting resource	Benefits	Draw-backs	Examples
Proof-of-work	CPU power (i.e. electricity)	Censorship-resistant and tamper-proof, strong immutability of record	Physical resource consumption (electricity), difficult to scale	Bitcoin, Litecoin
Proof-of-stake	Ownership of scarce tokens within the database	Energy-efficient, fast, easy to scale	Nothing-at-stake problem (casting a vote doesn't cost anything, which allows voting for different versions of the blockchain simultaneously)	NXT
Delegated proof-of-stake	Ownership of scarce tokens + peer reputation (elections for delegates)	Allegedly more efficient than PoS	Voter apathy in elections can leads to excessive centralization and reduced robustness	BitShares
Proof-of-activity (PoW/PoS-hybrid)	CPU power + ownership of scarce tokens	Combine some of the benefits of PoW and PoS	Still have some of the draw-backs of PoW and PoS	PeerCoin
Proof-of-burn	Destruction of scarce tokens within the database	Gives the benefits of proof-of-stake without any of its draw-backs	Difficult to build network effects and to implement before the blockchain is very mature	Counterparty
Proof-of-validation	Security deposit of scarce tokens subject to burn if voting dishonestly	Gives the benefits of proof-of-stake without almost any of its draw-backs	Nothing-at-stake problem still persists over long periods of time	Tendermint
Proof-of-capacity / Proof-of-storage	Free storage capacity (PoC) / Stored random data (PoS)	Energy-efficiency, speed	Physical resource consumption (wasted hard drive space) Nothing-at-stake problem exists, can morph into PoW	BurstCoin
Proof-of-importance	Participation in the economy (scarce tokens + transactional activity + peer reputation)	Tokens less likely to become concentrated to the point of crippling the entire system	Vulnerable to Sybil attacks, nothing-at-stake problem present on some level	NEM
Ripple protocol consensus algorithm	Peer reputation (Unique Node List)	Path-dependent consensus (fast, scalable and provable in state)	Unique Node Lists need to be actively maintained, network structure needs to be actively monitored	Ripple
Stellar consensus protocol	Peer reputation (Quorum vote)	Solves the nothing-at-stake problem without PoW	Initial tokens need to be manually disseminated	Stellar