Blockchain and cryptocurrencies technologies and network structures: applications, implications and beyond
Lisa Morhaim

To cite this version:
Lisa Morhaim. Blockchain and cryptocurrencies technologies and network structures: applications, implications and beyond. 2019. hal-02280279

HAL Id: hal-02280279
https://hal.archives-ouvertes.fr/hal-02280279
Submitted on 6 Sep 2019

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L’archive ouverte pluridisciplinaire HAL, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d’enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.
Blockchain and cryptocurrencies: Technologies and network structures: applications, implications and beyond

Lisa Morhaim*

Wednesday 4th September, 2019

Abstract

Blockchain technology is bringing together concepts and operations from several fields, including computing, communications networks, cryptography, and has broad implications and consequences thus encompassing a wide variety of domains and issues, including Network Science, computer science, economics, law, geography, etc. The aim of the paper is to provide a synthetic sketch of issues raised by the development of Blockchains and Cryptocurrencies, these issues are mainly presented through the link between on one hand the technological aspects, i.e. involved technologies and networks structures, and on the other hand the issues raised from applications to implications. We believe the link is a two-sided one. The goal is that it may contribute facilitating bridges between research areas.

Keywords: Blockchain, Cryptocurrency, Technologies, Network structures, Applications, Implications, Economics, Law, Geography, Humanities, Interdisciplinary research.

*University of Paris 2 Panthéon-Assas, CRED Paris Center for Law and Economics, Chaire Finance Digitale. Email: lisa.morhaim@u-paris2.fr.
## Contents

1 Introduction

2 Applications a brief sketch

3 Technologies, network structures and specificities
   3.1 Distributed system, peer-to-peer (P2P) network, decentralization and immutability
   3.2 Asynchrony, consensus and mining
   3.3 Cryptography, identity, anonymity and pseudonymity, privacy and security
   3.4 Platforms, architecture and design
   3.5 Trust
   3.6 Networks
   3.7 Multiplex networks, connecting blockchains and interoperability
   3.8 Economic analysis, networks and Blockchains: some insights towards new frameworks and models?
   3.9 Cryptocurrency and banking
   3.10 Markets
   3.11 Law

4 Beyond
   4.1 Risks
   4.2 Adoption, digital divide, digital culture and education
   4.3 Quantum computing and Blockchain, Quantum Blockchains, Quantum networks
   4.4 Sustainability and energy consumption

5 Conclusion
1. Introduction

Blockchain technology is bringing together concepts and operations from several fields, including computing, communications networks, cryptography, and artificial intelligence (Swan[547]). Additionally, the separation between economics’ analysis, law analysis, etc can not be quite pertinent as they often mix. The Blockchain technology has broad implications and consequences thus encompassing a wide variety of domains and issues. Network Science is a deeply interdisciplinary rooted field. Keeping in that tradition, this paper proposes some paths to think about the Blockchain revolution and analyze its technologies and structures, applications and implications in a deeply interdisciplinary way.

The objective is mainly twice: to give a most possible synthetic panorama of issues raised by the Blockchain technologies and network structures both for researchers working on a specific Blockchain research area and for researchers working and thinking on the tools in one or some of the specific domain(s) that are in the scope of the paper (which includes besides Network Science, economics, but also computer science, law, geography, political science, etc) and we hope it will easy and enhance interdisciplinary researches. As the paper is intended to easy bridges between area researches, it has been conceived somehow self-contained and synthetic as possible.

The aim of the paper is to provide a synthetic sketch of issues raised by the development of Blockchains and Cryptocurrencies. These issues are mainly presented through the link between on one hand the technological aspects (involved technologies and networks structures) and on the other hand the issues raised in Economics, Law, etc, from applications to implications and beyond. We believe the link is a two-sided one. The goal is to contribute facilitating bridges between research areas and to give a first introduction to these links and issues. It refers to many existing good surveys and on-going research.

The panorama have been thought from the issues they raise and discuss. Given the fast rythm at which new articles and analysis are provided, it is becoming impossible to cover exhaustively the literature on Blockchain, cryptocurrencies and related fields. Choices have been made in order to provide a quite wide range of questions and issues that are being currently discussed while easying interdisciplinary research. Network Science is rooted as an interdisciplinary field using and providing mathematical, physical, statistical as well as biological, engineering and computer science tools. As the Blockchain technology field is spreading, it is becoming clearer and clearer that Network Science can deeply fruitfully provide and develop tools at the interaction with some other various disciplines, as Economics, Law, Geography, History, Anthropology, Sociology, Political Science, etc....The aim of this paper is to give insights on what such an experience is already being done while providing some motivation and will for future research, mainly through a few chosen examples and studies. The main remarkable feature of blockchain technology is that it has been thought so that the users trust the system without no longer having to trust the partner or an intermediary and so that it solves the double-spending\(^1\) issue.

Cryptocurrency\(^2\). As reported by the ECB-European Central Bank[47, 48], Virtual Currency Schemes (VCS) are diverse, ECB distinguishing closed, unidirectional, and bi-directional VCS while underlying that the most common approach distinguishes centralised and decentralised VCS. Decentralised bi-directional VCS (the vast majority of all VCS) can differ from various standpoints.\(^4\) The virtual currency ecosystem involves new categories of actors not before present in the payments

\(^1\)i.e. spending the same unit more than once.

\(^2\)Cryptocurrencies date from Chaum 1983[136] and many developments have followed (see [496]). Haber Stornetta 1990[256], referring to Diffie Hellman[177]’s asymmetric (i.e. public-key) cryptography\(^3\) (see also RSA[491], Merckle[391], Bayer Haber Stornetta[59]), first described the concept of a blockchain.

\(^3\)ECB[47, 48]. They can differ from their validating systems (i.e. the methods used for validating the transactions made and securing the network), the algorithms involved (i.e. the mathematical procedure for calculating and processing data), their (total) supply of coins, a functional perspective (i.e. extra features available on the network).
environment. Since Nakamoto’s seminal paper on Bitcoin, the Blockchain technology is currently intensively studied in the scientific community. As Swan underlines: Bitcoin terminology can be confusing because the word Bitcoin is used to simultaneously denote three different things. First, Bitcoin refers to the underlying blockchain technology platform. Second, Bitcoin is used to mean the protocol that runs over the underlying blockchain technology to describe how assets are transferred on the blockchain. Third, Bitcoin denotes a digital currency, Bitcoin, the first and largest of the cryptocurrencies.

Blockchain and cryptocurrencies: definitions, technologies and specificities A blockchain is the combination of several technologies and characteristics: distributed database over a P2P network, public-key cryptography (including eventually digital signature) and eventually consensus mechanisms (see Narayanan Clark). Narayanan Clark show that, in 2008 when Nakamoto’s paper on Bitcoin was published, nearly all of the technical components of bitcoin originated in the academic literature of the 1980s and ’90s. For a discussion on public blockchain versus private (and semi-private) blockchain see Guegan.

A cryptographic hash function $h$ is firstly a hash function i.e. one that maps a bit string $x$ (of arbitrary length) to a short unique value $h(x)$ (a short bit string of fixed length) such that computing $h(x)$ knowing $x$ is easy. Given a hash function $h$, a collision is a couple $(x, x')$ such that $x \neq x'$ and $h(x) = h(x')$. A cryptographic hash function $h$ is collision resistant, i.e. it is infeasible to find a collision. It is a one-way function: finding $x$ from its hash value $h(x)$ is infeasible. It is expected to satisfy the avalanche effect: a small change in $x$ must lead to a large change in $h(x)$.

Public-key (or asymmetric) cryptography is a cryptographic system that involves the use of two keys, a public-key that may be disseminated widely by the owner and a private key known only to the owner (and that must remain private to achieve effective security). The key used to encrypt the message cannot be used to decrypt it, and the message encrypted using one key can only be decrypted with the other key. It can ensure confidentiality, the message (data) being encrypted by the sender with the recipient’s public key and decrypted by the recipient with the recipient’s private key. It can ensure authentication and data integrity through digital signatures, the message being encrypted by the sender with her/his own private key and decrypted by anyone with the sender’s public key.

Combining public-key cryptography and hash functions allows to ensure both authentication and confidentiality efficiently.

A blockchain is a distributed ledger (i.e. a distributed database allowing to record and share data across multiple data stores, the ledgers) with a linked list of blocks using hash pointers (i.e. pointers to where some information is stored, together with a cryptographic hash of the information), such that additions to the database are done through the procedure

---

5 These are (ECB[47, 48]): inventors (known or unknown individuals or organisations that create a virtual currency and develop the technical part of its network), issuers (that are able to generate units of the virtual currency), miners (persons, sometimes working as a group, who voluntarily make computer processing available in order to validate a set of transactions (a block) made with a decentralised VCS and add this to the payment ledger (a blockchain)), processing service providers (facilitating the transfer of units from one user to another, these services being part of the activity performed by the miners in decentralised VCS), users, wallet providers (offering a digital wallet to users for storing their virtual currency cryptographic keys and transaction authentication codes, online or offline wallets, although users can also set up and maintain a wallet themselves without making use of a wallet provider), exchanges offer trading services (quoting exchange rates by which the exchange will buy/sell virtual currency against the main currencies), trading platforms (that function as marketplaces) and various other actors not specific to the VCS environment (merchants, payment facilitators, software developers, computer hardware manufacturers (building specific equipment for mining) and ATM-Automated Teller Machine manufacturers).

6 See also Sherman

7 meaning here that no process, not even one subject to arbitrary faults, can find a collision (Cachin Guerraoui Rodrigues[112]). In particular, it does not mean that no collision exists. This can also be expressed in terms of “easy/not easy” and is clearly related to algorithmic complexity issues (see Katz et al.[317, 316], Stallings). h being clearly not continuous nor invertible.

8 Each user will thus have a collection of public keys of the other users

---
transactions are grouped with other transactions to form a block

- the network nodes determine collectively if the block is valid through a validation algorithm called a consensus mechanism

- as an example, in the PoW consensus mechanism, a puzzle that needs time and computing power has to be solved. The miner who first solves the puzzle sends the solution to the other nodes of the network (who can easily check it and validate the transactions in the block), and is rewarded for his contribution to the network by finding the puzzle solution.

- once a block (each block containing the transactions, a hash of its own, a hash of the previous block, timestamp) is validated, it is added to the database and the blockchain is updated across the network.

**Do you need a blockchain?** *Blockchain is not advantageous for every situation. On the way to construct indicators for comparing Blockchains. A decision-model. A vademecum on Blockchain for identifying when, which and how. Framework propositions for practitioners and decision-tree. On DLT characteristics. On misconceptions. Insights to select a protocol.*

As noted in Swan[547]: the Blockchain is not for every situation despite the many interesting potential uses of blockchain technology, one of the most important skills in the developing industry is to see where it is and is not appropriate to use cryptocurrency and blockchain models (Swan[547]). So, firstly, do you need a Blockchain? (see Wust[595]) or what blockchain alternative do you need? (see Koen[330]). Criteria are being developed. Guegan Henot[250] analyse from different aspects why a company (in banking or insurance system, and industry) interested to develop its business with a public blockchain decides that a blockchain protocol is more legitimate than another one for the business it wants to develop looking at the legal (in case of dispute) points of view and introduce the notion of probative or evidential value associated to a blockchain in order to provide to the entrepreneurs an intrinsic value characterizing the blockchain he/she wants to use to develop his/her business. By quantifying the revenues a 51% attack can create for the miners, a corresponding cost is provided for each blockchain. Betzwieser 2019[77] propose a decision model for the implementation of Blockchain solutions. Belotti et al.[65] provide a vademecum on Blockchain technologies, drawing a picture to answer to when (when there are actual advantages in using blockchain instead of any other traditional solution, such as centralized databases), which (which kind of blockchain better meets use-case requirements) and how (how to use it). De 2019[170] propose a framework of blockchain models to help practitioners understanding and potentially implement Blockchain-based solutions based. Mulligan[409] propose a framework for practitioners (including a decision-tree). Kannengiesser et al.[313] present a comprehensive set of 49 DLT characteristics synthesized from the literature on DLT, which have been found relevant to consider when developing viable applications on DLT. Conte[154]'s purpose is to clarify current and widespread misconceptions about the properties of blockchain technologies. Shahaab[520] have listed consensus protocols against basic features and sector preference in a tabular format to facilitate selection. They argue that no protocol is a silver bullet, therefore should be selected carefully, considering the sector requirements and environment.

**Applicability.** *An applicability framework. A taxonomy of Blockchain applications.*

Risius and Sohrer[488] provide a framework to understand where and how blockchain technology is effectively applicable and where it has mentionable practical effects. Labazova[346] gives a taxonomy of blockchain applications.

**Layers** *Some analysis of Blockchain through layers.*

A blockchain can be analyzed through its layers (see Singhal et al.[532]): application layer (i.e. the layer where the desired functionalities are coded and made an application out of it for the end users), execution layer (i.e. the layer where the executions of instructions ordered by the application layer take place on all the nodes in a blockchain network, the instructions being simple instructions or a set of multiple instructions in the form of a smart contract), semantic layer (the rules of the system
can be defined in this layer, such as data models and structures and how the blocks are linked with each other), propagation layer (i.e. the peer-to-peer communication layer that allows the nodes to discover each other), consensus layer (i.e. the layer getting all the nodes to agree on one consistent state of the ledger). See also Casino[125]. Glaser Hawlitschek Notheisen in [189] (volume 1 chapter 4) investigate the blockchain as a platform and present technical layers of the system as well as institutional characteristics and governance implications, followed by a discussion of the role of trust in blockchain systems.

**Digital disruption** *Thinking the Blockchain revolution within innovations (and digital) disruption*

Theories of disruptive innovations and managerial implications have been explored and developed since the 1990’s. Moller[405] on characterizing digital disruption in the theory of disruptive innovation. See also Lessig[353, 354], Wu[594], De Filippi Hassan[166], De Filippi Wright[169], Olleros[435].

**On previous and existing surveys**

**Books** Many books on Blockchain have been published. See Narayanan et al. 2016[415], Tapscott[554], Casey[124], Burniske[109], Swan[547], Ammous 2018[20],Campbell-Verduyn [118], Treiblmaier Beck[189], etc. On Blockchain economics: see Tasca 2016[556], Swan[549] and the references herein, and Blockchain and the law: see De Filippi Wright[169].


**Organization of the paper.** Section 1 introduces the aims, definitions, literature and frameworks.
Section 2 provides a brief sketch of some of the many Blockchain applications. Section 3 describes the technologies, specificities, network structures, implications and related issues of Blockchains and Cryptocurrencies. Section 4 provides some insights on a broader scope. Section 5 concludes.

2. Applications a brief sketch

For a systematic literature review of Blockchain-based applications refer to Casino[126].

In the economic areas, one can insist on Fintech (see Kavuri 2019[318], Anand 2019[25]), Business (see Viriyasitavat et al.[573] investigate the characteristics of Blockchain and business processes), Tourism (see Horst et al. (volume 2 chapter 1 in Treiblmaier Beck 2019[189]), Intellectual property, Industries (see Al-Jaroodi[9]), Payments industry (see Holotiuk et al. (volume 1 chapter 7 in [189]), including a discussion agenda based on pain points and opportunities), Music industry, ICO Crowdfunding and Microfinance (see Boreiko[98] describes all important aspects of Blockchain financing and provide a comparative study of token sales versus crowdfunding and conventional financing methods, provide a review of literature on token sale financing and challenges and provide empirical related studies, Li 2019[356] for a recent discussion on ICO current research and future directions, Fridgen[220] for a taxonomy blockchain and crowdfunding, Arnold et al.(volume 1 chapter 8 in Treiblmaier Beck 2019[189]) on identifying industries and use cases that may benefit from adopting blockchain when it comes to crowdfunding and showing how crowdfunding and initial coin offerings differ and how the latter is reshaping the former, Cerviello[131] for statistical approach to detect characteristics of ICO significantly related to fraudulent behaviors, Holoweiko 2018[279] on ico security, Garratt garratt2019entrepreneurial examines how financing a start-up through an ICO changes the incentives of an entrepreneur relative to debt and venture capital financing: depending on market characteristics, an ICO can result in a better or worse alignment of the interests of the entrepreneur and the investors compared with conventional modes of financing), Humanitarian aid, Shared Economy (see Huckle[291] (volume 1 chapter 3 in[189]) providing a technology adoption perspective on the Blockchain-Based decentralized business models in the sharing economy and apply agent-based modeling to explore the circumstances under which a decentralized sharing economy business model might achieve widespread adoption), Management and governance (DAO, dApps, Howell 2019[286], Young 2018[605]), Supply Chain (see [576]), Supply Chain Finance (see [278]), Marketing and Advertising uses.

In Law areas (see references in Bolotaeva[94], Filippi Hassan[169], De Filippi[169], one can insist on Smart Contracts (SCs) (see Bakos Halaburda 2019[46], Howell 2019[286], see Alharby Moorsel[10], see also[87, 268, 176], Meneghetti[390], senopra[347], [426], see Dargaye[162]10, Tonelli[564], Casino[125], Marchesi Tonnelli[461], Krishnan [335] on smart contract and interoperability, O’Sheilds[438] and Westerkamp[584]), Multisignature: Smart Complex Contracts, LegalTech (see Corrales Fenwick Haapiaio[156]), Regulation (see Smith[534] for a framework, Melo[387], Baidoo[45]), Dispute resolution (Raymond 2014[480]), Crowdsourcing and Court system (Ast[35], Li 2018[358]).

Beside Economics and Law, many other applications are being developed: Archives (on decentralized scientific publications, see Tenorio 2019[560] and on medical see Coghill[150]), Health (see Burniske 2016[592], Sachin et al. (volume 2 chapter 5 in [189]) presenting a mobile healthcare system for personal health data collection, sharing, and collaboration between individuals and healthcare

10Dargaye[162] presents a formal logical framework able to extend the execution of blockchain transactions to events coming from external oracles: in many industrial applications smart contracts react to information coming from external sources (sensors, human interfaces, other applications), often called oracles in the blockchain jargon, which amplifies their vulnerability, these events being by essence non-reliable, since transaction execution can be triggered by information whose veracity cannot be established by the blockchain
providers, as well as insurance companies, Genestier[226], review[339, 238, 185, 616, 320, 295, 333]), Agriculture, Food traceability, Energy (see Strucker et al.(volume 2 chapter 2 in Treiblmaier Beck 2019[189]) having a close look at the energy sector and present some ideas on how blockchain might potentially impact this sector in the not-so-far-off future, Peter[455]), Politics (see De Filippip Loveluck[168], Berg[76], Martinez[382] argues on Blockchain solution in eDemocracy platforms, Grontas[240] on electronic voting, Dhillon Grammateia Riley[175] on voting questions for economists, Elsden[199]), Education (see Chen [138], Sommer[537], Palavinel[448]), Post-Disaster Recovery (see Nawari Ravindran[418], Demir[172]), Smart cities (see Kitchin[325], Speed[539], Ramos 2019[475]), Prediction markets, Blockchain gaming (see Min[401], and Min[400] on security of blockchain games).

3. TECHNOLOGIES, NETWORK STRUCTURES AND SPECIFICITIES

Technical aspects and specificities and related issues involved in applications and implications reveal that advantages of Blockchain can sometimes also be their main limitations.

3.1 DISTRIBUTED SYSTEM, PEER-TO-PEER (P2P) NETWORK, DECENTRALIZATION AND IMMUTABILITY

3.1.1 DISTRIBUTED SYSTEM, PEER-TO-PEER (P2P) NETWORK AND BLOCKCHAIN

*Distributed system. Processes cooperate? Distributed computing community. Theoretical aspects of Blockchains.*

Blockchain protocols are solving a classical distributed computing problem. When a program encompasses multiple processes (a process representing a computer, a processor in a computer, etc), the fundamental problem is having all the processes cooperate on a common task. Important issues then arise as the tolerance to uncertainty and adversarial influence in a distributed system, which may arise from network delays, faults, or even malicious attacks (Cachin Guerraoui Rodrigues[112]). There is growing work on the line of recent distributed computing community efforts dedicated to the theoretical aspects of blockchains (see [28, 468, 251]). Anceaume et al.[26] is the first paper specifying blockchains as a composition of abstract data types all together with a hierarchy of consistency criteria that formally characterizes the histories admissible for distributed programs that use them. Anceaume et al.[27] introduce the Distributed Register, a register that mimics the behaviour of the Bitcoin ledger, the aim being to provide formal guarantees on the coherent evolution of Bitcoin. Rauchs et al.[478] establish a conceptual framework and terminology that can be applied across DLT systems and to distinguish these newer technologies from traditional databases and other systems, providing a multidimensional tool for examining and comparing existing DLT systems and their traits and features, it also can serve when examining new DLT systems proposals. Siris et al.[533] discusses on the interledger approach: blockchains and more generally distributed ledger technologies(DLTs) shortcomings becoming more apparent, a relatively recent approach to address their performance, scalability, privacy, and other problems are to use multiple different DLTs instead of relying on just one. Daniel Burkhardt et al. (volume 2 chapter 4 in [189]) argue that distributed ledgers will enable new opportunities to replace existing components on all layers of industrial IT architecture.

The main examples of distributed systems without blockchains are distributed systems based on

---

11see Cachin et al.[112], Fokkink[216, 215]

12Anceaume et al.[27] underlines that even though the behaviour of distributed ledgers is similar to abstractions that have been deeply studied for decades in distributed systems no abstraction is sufficiently powerful to capture the distributed ledger behaviour.
Directed Acyclic Graph (DAG). Instead of a chain, such distributed systems use a Directed Acyclic Graph (DAG)\textsuperscript{13} as decentralized structure. Examples of such cryptocurrencies are Iota (based on the DAG called Tangle), Hashgraph, and Nano. There are other distributed systems without blockchains, for example Corda\textsuperscript{[270, 106, 105]} used to treat financial legal agreements could look like a firms’ consortium blockchain but uses of a concept of change of states and transactions in place of chain of blocks.

3.1.2 Decentralization

Distributed system and organization. New forms of organization. Institutional cryptoeconomics. Dynamics. Organizational economics

Resnick\textsuperscript{[487]} discusses how computer-modeling activities can help people move beyond the centralized mindset, helping them gain new insights into (and appreciation for) the workings of decentralized systems. Blockchain can be thought of as an institutional innovation. Berg\textsuperscript{[75]} introduces the V-form organisation, a new form of firm organisation where vertical integration is outsourced to a decentralised distributed ledger (a blockchain), and rely on the coordination of a (trusted) third party. Allen\textsuperscript{[12]} apply institutional cryptoeconomics to the information problems in global trade, model incentives under which blockchain-based supply chain infrastructure will be built, and make predictions about the future of supply chains, arguing blockchain will change the patterns and dynamics of how, where and what we trade through four main reasons. Berg\textsuperscript{[73]} study the institutional economic dynamics of a wide-spread blockchain technology adoption, examining the structural economic effects of this institutional innovation as disintermediation in markets, dehierarchicalisation of organisations, and growing private provision of economic infrastructure for exchange, contracting and coordination. Schneider\textsuperscript{[509]} discusses the very concept of decentralization, arguing that to be a reliable concept, it should come with high standards of specificity. Takagi\textsuperscript{[553]} study the economic mechanisms behind blockchain-enabled decentralisation from the viewpoint of organizational economics.


See Tasca et al.\textsuperscript{[557]}: Consensus Network Topology describes the type of interconnection between the nodes and the type of information flow between them for transaction and/or for the purpose of validation. Consensus Network Topology is linked to the level of (de)centralisation in the validation process, though it is not the only determinant as other factors influence it (like the reward mechanism) (see Bonneau et al.\textsuperscript{[96]}). Gencer et al.\textsuperscript{[225]} study decentralization metrics in Bitcoin and Ethereum networks, adapting Internet measurement techniques. Kwon et al.\textsuperscript{[342]} define \((m, \varepsilon, \delta)-decentralization\), a state satisfying that there are at least \(m\) participants running a node, and the ratio between the total resource power of nodes run by the richest and the \(\delta\)-th percentile participants is less than or equal to \(1 + \varepsilon\). So that when \(\delta = \varepsilon = 0\) and \(m\) is large enough, \((m, \varepsilon, \delta)-decentralization\) is full decentralization. Stifter\textsuperscript{[543]} shows an example of data mining applied to the analysis of the blockchain network. Bodo\textsuperscript{[93]} analyzes decentralization related to distributed ledger technologies (DLTs), its extent, its mode, the systems which it can refer to as the products of particular economic, political, social dynamics around and within these techno-social systems. Chu Wang\textsuperscript{[147]} explore the trade-off decentralization-scalability, decentralization being quantified by the decentralization level they define within the paper. Cong et al.\textsuperscript{[152]} study the centralization and decentralization forces in the creation and competition of mining pools.

\textsuperscript{13}i.e. une chaîne avec des ramifications
Dapps (decentralized applications), DAOs (decentralized autonomous organizations), DACs (decentralized autonomous corporations) and DASs (decentralized autonomous societies)

See Raval[479] for more details on Decentralized Applications. Hsieh[287] analyse Bitcoin as an example to shed light on how a DAO works in the cryptocurrency industry.


Swan[547] already notes that “There is a mix of forces both toward centralization and decentralization operating in the blockchain industry”. Hsieh et al.[288] provide a statistical analysis whose results may seem paradoxical: they find that decentralization at the blockchain level affects returns positively as one would expect, since the promise of blockchain is decentralization as a way to create value but also find that decentralization at both the protocol and organizational levels affects returns negatively. Neitz[420] provide a discussion on Blockchain, decentralization issues and the role of the Law.

3.1.3 Record-keeping and immutability


As immutability (if realized) is also irrevocability: there is ongoing research on solving this conflict, among which Politou et al.[466]’s survey on mutability challenges, Ateniese et al.[36] who give a framework that makes it possible to re-write and/or compress the content of any number of blocks in decentralized services exploiting the blockchain technology, Kuhn[337] proposing a data structure for integrity protection with erasure capability, Florian[214] providing a discussion of legal and non-legal reasons for local erasure and proposing an approach enabling nodes to erase data while continuing to store and validate most of the blockchain, and on Blockchains and Rgpd see Pagallo et al.[446], Jussila[308].

3.2 Asynchrony, consensus and mining

3.2.1 Asynchrony

Coordination. Asynchrony. Double-spending. Is consensus necessary?

Coordinating the actions of processes is crucial for virtually all distributed applications, especially in asynchronous systems (Aspnes[34]). As discussed in Guerraoui[472]: there seems to be a common belief that consensus is necessary for solving the double-spending problem, whether it is for a permissionless or a permissioned environment, the typical solution uses consensus to build a totally ordered ledger of submitted transfers. Guerraoui[472] show, by introducing AT2 (Asynchronous Trustworthy Transfers) a class of consensusless algorithms, that this common belief is false: consensus is not needed to implement a decentralized asset transfer system.

3.2.2 Consensus mechanisms

A consensus mechanism can be thought as a mechanism to confirm a person’s innocence or to discourage him/her to act wrong. The incentives to act not wrong are quite different concepts through computer science, economic or law lenses.


Guerraoui et al.[252] provide a unifying scheme that captures at a high level the behavior of any blockchain protocol, discussing which variation opens which vulnerability breach. Garay Kiayias[223] in a consensus taxonomy give a roadmap for studying the consensus problem under its many guises,
classifying the way it operates in the various settings and highlighting the exciting new applications that have emerged in the blockchain era. Rigorous formalization of specific blockchain protocols and their properties can be found in Badertscher et al.[44], Pass et al. [453], Garay et al.[222].

The blockchain community does not have well-established theoretical foundations for consensus algorithms although Sorensen[538] establishes a framework intended for academic and industrial blockchain researchers as a foundation for the theory of consensus. See Cachin Vukolić[114], Cachin[113], Xiao et al.[596] for a recent survey of distributed consensus protocols for Blockchain networks. Ehmke Blum Gruhn[190] study properties of decentralized consensus technology (“why not every Blockchain is a Blockchain”). See Amoussou[24] on blockchains based on repeated consensus. Shahaab[520] review 66 known consensus protocols and classify them into philosophical and architectural categories, they argue that advancement of consensus protocols in recent years has enabled distributed ledger technologies (DLTs) to find its application and value in sectors beyond cryptocurrencies. see Wang[581] for a survey on consensus mechanisms and mining strategy management in blockchains. See Azouvi Hicks Murdoch[40] for a discussion on the role of incentives in consensus mechanisms and Hicks Murdoch[274]. See also Azouvi Hicks[39] for a discussion on game-theoretic tools.

Consensus algorithms are numerous, and some are being created, among which: Proof of Authority (PoA), Proof of Work (PoW) (see Saleh[500] for economic impact analysis, see also Szalachowski[552]), Proof of Stake (PoS) (see Nguyen[425], Barinov[49]), Hybrid PoW/PoS, Delegated Proof of Stake (DPoS) Proof of Brain, Proof of Retrievability (PoR), Proof of Importance (PoI), Byzantine Generals Problem and Practical Byzantine Fault Tolerance (PBFT) (see for instance Amoussou et al[22] modelling the Byzantine-consensus based blockchains as a committee coordination game), Proof of Burn (also examined in Saleh[500] for economic impact), Proof of Activity, Proof of Capacity, proof of storage, Proof of Elapsed Time (PoET), Simplified Byzantine Fault Tolerance (SBFT), Proof of concept, DAG, Committee selection, RAFT consensus (see Huang[289]), Chan et al. 2019[134] propose a State Machine Replication (SMR) protocol (i.e. consensus protocol) inspired by a social phenomenon called herding, where people tend to make choices considered as the social norm. Partially synchronous protocols are being developed see Ranchal-Pedrosa Gramoli[476] that develops latypus, a partially synchronous offchain protocol for blockchains, etc

3.2.3 Mining and mining pools, fees, costs, incentives and strategies


Bitcoin pooled mining reward systems have been analyzed by Rosenfeld[497], describing various scoring systems used to calculate rewards of participants in Bitcoin pooled mining, explaining problems each were designed to solve and analyzing their respective advantages and disadvantages. Wang et al.[581] survey on consensus mechanisms and mining strategy management. One can refer to Zhu et al.[614] for a (quite modelized) survey on reward distribution mechanisms and withholding attacks in Bitcoin pool mining. Romiti[495] provide an empirical analysis of Bitcoin mining shares, analyzing mining reward distribution within three of the four largest Bitcoin mining pools and examine their cross-pool economic relationships, their results (in line with previous research) suggesting centralization tendencies in large mining pools and cryptocurrencies in general. Chatzigiannis[135] present a mining portfolio model, miners optimally distributing their computational power over multiple pools and PoW cryptocurrencies taking into account their risk aversion levels, while Wang Tang[582] model the pool mining process as a two-stage game, and Kitt[327] on allocating rights for mining as a contest. Eyal Sirer[203] showed that the Bitcoin network is vulnerable even if only a small portion of the hashing power is used to cheat (“selfish mining strategy”) and that unless certain assumptions are made, selfish mining may be feasible for any group size of colluding miners. The Bitcoin mining protocol is not incentive-compatible, as they present an attack with which colluding miners obtain a revenue larger than their fair share. They propose a practical modification to the Bitcoin protocol that protects Bitcoin in the general case that prohibits selfish mining by
pools that command less than 1/4 of the resources. Selfish mining have been generalized (algorithm to find $\varepsilon$-optimal strategies in [504], stubborn mining in [419], multiple selfish miners in [349], etc) and Grunspan Pérez-Marco[242, 244, 243] have recently proposed a profitability model for repetition games, finding that in the bitcoin network, no strategy is more profitable than the honest strategy before a difficulty adjustment, so selfish mining can only become profitable afterwards, and thus being an attack on the difficulty adjustment algorithm. Falk et al.[206] study blockchain-based platforms that have implemented token weighted aggregation to incentivize efficient and effective information crowdsourcing from their users in a decentralized way (these systems aggregate information through user votes, where the final action of the system is determined based on the weighted average of the users votes, and each users vote is weighted according to his token holdings within the system) and provide economic analysis including on wether token weighting encourages or discourages truthful voting and how accurate is the resulting crowdsourced information. Brown-Cohen et al.[107] focus on incentive-driven deviations (any participant will deviate if doing so yields higher revenue) instead of adversarial corruption (an adversary may take over a significant fraction of the network, but the remaining players follow the protocol), obtaining several formal barriers to designing incentive-compatible proof-of-stake cryptocurrencies (that don’t apply to proof-of-work). Liu[363] provides a viewpoint on research on token incentive mechanism of open source project taking Blockchain project as an example. Prat Walter[469] propose an equilibrium model of the market for Bitcoin mining, refer also to their paper for the main related literature. Zamyatin et al. [608] formulate a model of the dynamics of a queuebased reward distribution scheme in a popular Ethereum mining pool and develop a corresponding simulation. Bissias et al.[86] find that there exists a resource allocation equilibrium between any two blockchains, which is essentially driven by the fiat value of reward that each chain offers in return for providing security and that this equilibrium is singular and always achieved provided that block producers behave in a greedy, but cautious fashion while the opposite is true when they are overly greedy: resource allocation oscillates in extremes between the two chains. Bissias et al.[85] present an economic model that leverages Modern Portfolio Theory to predict a miners allocation over time using price data and inferred risk tolerance. Shanaev et al.[524] test theories of cryptocurrency pricing (causal inferences from the instrumental variable approach on the marginal cost of mining, Metcalfe’s law and cryptocurrency value formation). Hinzen[275] provides discussion on Proof-of-Work’s latency dilemma and a permissioned alternative.

3.3 CRYPTOGRAPHY, IDENTITY, ANONYMITY AND PSEUDONYMITY, PRIVACY AND SECURITY

3.3.1 BLOCKCHAIN CRYPTOGRAPHY

Bonneau Miller[95] discusses on cryptocurrency without public-key cryptography and provide a comparison with Bitcoin, having economic implications (in particular it could involve thinking and distributing fees differently). Wang et al.[580] survey cryptographic primitives of 30 principal cryptocurrencies. Raikwar[473] beside reviewing and systematizing the cryptographic concepts already used in blockchain, give a list of cryptographic concepts which have not yet been applied but have big potentials to improve the current blockchain solutions and include possible references of these cryptographic concepts in the blockchain domain. They postulate 18 challenging problems that cryptographers interested in blockchain can work on.

3.3.2 IDENTITY, ANONYMITY AND PSEUDONYMITY, AND PRIVACY

For a fundamental paper, refer to (previous to blockchain) Sweeney[550] and for a discussion on an algorithmic introduction to anonymity in asynchronous systems, see Raynal[481], distinguishing process-anonymity and memory-anonymity. See also Herrera-Joancomart Jordi [273], Fabian[204],
While studying Bitcoin, Moser Bohme surveys and compares transaction anonymization techniques. Moser argues that as all transactions in the network are stored publicly in the blockchain, allowing anyone to inspect and analyze them, the system does not provide real anonymity but pseudonymity. Community detection tools have been used in Cazabet et al. to argue that studying the Bitcoin transaction network, such tools can be used to re-identify multiple addresses belonging to the same user. Dunphy et al. review open questions and challenges for distributed ledgers on decentralizing digital identity. Lesavre propose a taxonomic approach to understanding emerging Blockchain identity management systems. Borgonovo on Privacy. Bushager provide a study of users experiences of bitcoin security and privacy.

3.3.3 Security

For a survey see Conti. See also Saad et al. developing defense strategies in their overview on attacks in Blockchains. For a recent survey on blockchain from a security perspective see Dasgupta. Bushager provide a study of users experiences of bitcoin security and privacy. Manuskin et al. introduce Ostraka, a blockchain node architecture that scales linearly with the available resources, i.e. to secure Blockchain scaling by node Sharding. see also network analysis. On ico security, see Holoweiko. In order to lay down the foundation of a common body of knowledge, Zhang Preneel introduce a multimetric evaluation framework to quantitatively analyze PoW protocols chain quality and attack resistance. See also Azouvi for SoK tools for game theoretic models of security for cryptocurrencies.

3.3.4 Data Security and Privacy

Two-sided issue: issues one side on Data Security and Privacy when using Blockchains and another side on using Blockchain technology for Data Security and Privacy. Truong propose a Blockchain-based Solution for GDPR-Compliant Personal Data Management. On Blockchain for data provenance Tosh. See Clementi for an example on securing the sharing of Flight Data. On privacy issues when using Blockchains in Smart Cities, see Ramos et al. Wang describe a blockchain based privacy-preserving incentive mechanism in crowdsensing applications. See also Daneshgar, Alsayed and in Casino the section on Data management and privacy and security solutions.

3.4 Platforms, architecture and design

Blockchain-based platforms. Blockchain as a platform. Architecture. Design. Scalability. Velocity. On platforms based on distributed ledger technology see Schoenhals for an overview, on Blockchain as a platform Glaser, Sarkintudu for a taxonomy of blockchain platforms. See also De Filippi. Constantides have edited research to discuss platforms and infrastructures concomitantly. Glaser et al. (volume 1 chapter 4 in) investigate the blockchain as a platform and present technical layers of the system as well as institutional characteristics and governance implications, followed by a discussion of the role of trust in blockchain systems. On scalability see Szabociteszabo money, Jiao. Dang et al. study the use and effectiveness of trusted hardware on scaling distributed consensus protocols. Duffie examine monetary policy implications and business strategy concerns related to the introduction of digital currencies and faster payment systems. Lei prove that the blockchain concept helps to shorten the key transfer time.
3.5 Trust

The implications of the Blockchain technology could be at very various levels, because it modifies trust and trust is central to many interactions. Trust have been studied across many different disciplines. Thielmann Hilbig[561] provide a review on interpersonal trust among strangers accross many disciplines (including psychology, economics, political science, sociology, law). Tazdait[559] provides insights for a study of the economic analysis of trust. Note that this must include also issues about trust in technical systems (see Kaindl Svetinovic[310] arguing that both undertrust and overtrust need to be avoided). Glaser et al. (volume 1 chapter 4 in [189]) investigate the blockchain as a platform and present technical layers of the system as well as institutional characteristics and governance implications, followed by a discussion of the role of trust in blockchain systems. See also Kim[323] and references herein.Trust, IoT and network analysis see Li[357]. Mistrust see Tariq 2019[555]. Kaindl Svetinovic[310] analyse whether new systems can be trusted by human users through the notions of Undertrust and Overtrust.

3.6 Networks

3.6.1 Networks, Community structures, Hierarchies and digital geographies


On one hand, community structures14 ([424]), including topological properties of the communities (see Orman et al.[437]), are one of the most relevant key features in the study of real-world complex networked systems, let them be considered as static or temporal (see [130]) and has many application areas (see Karatacs[315]): for a review and discussion on community structure see Cherifi et al.[142]. Moreover, as underlined by Ghalmane et al.[227] identifying influential spreaders in networks is an essential issue: they introduce a framework allowing to redefine all the classical centrality measures (designed for networks without community structure) to non-overlapping modular networks and extend some centrality measures to networks with overlapping communities, as in real-world networks, nodes usually belong to several communities. This can be completed with many other tools, including core decompositions (see Malliaros 2019[378]), etc.

On another hand, maps can be defined as graphical tools that “classify, represent and communicate spatial relations; a concentrated database of information on the location, shape and size of key features of the landscape and the connections between them” (Hodgkiss cited in [528]). In their (beautiful) Atlas of Cyberspace, Dodge Kitchin[181] give insights on the way cyberspace has evolved and provide cyberspace representations (maps, diagrams, etc) while explaining the informations considered, cartography goals and the mapping techniques. They also examine critically such maps in [180]. In Abrams Hall[4] an analysis of mapping as new cartographies of networks and territories is provided while in Dodge Kitchin Perkins[183] are developed many aspects15 of new mappings. Landscape research (see Hunziker et al.[294]) is developing tools dealing with the multi-faceted interrelationship between landscape and society, and digital geographies examine the spread of digital devices, platforms, and code as they infiltrate, define, and shape the spaces and experiences of all human and animal life (Gieseking[229]). See also Hirschkon[276] on Blockchain and traditional Nation-State relationships.

Historically oriented social network analyses as developed by Padgett Powell[445, 445] or Ferguson[210, 211] show that the emergence of organizational novelty comes from spillovers accross intertwined mul-

---

14See also Estrada[200, 201, 202], Konig Battiston[394], Tasca Tessone[557], Newman Watts Barabasi[423].

15Noting that “The power of a map lies in how it communicates spatial relations, how the information has been selected, abstracted, generalized and portrayed by the cartographer. Because of this process of creation, no map is an objective, neutral artefact as many subjective decisions are made about what to include, how the map will look, what the map is seeking to communicate” ([183])
tiple networks and hierarchies. This is also the kind of issues that are raised through topological thinking in social sciences and geography (Allen[14, 17, 15, 16], Paasi[444]). Via a reading of Steven Soderbergh’s 2011 film, Contagion, Dixon et al.[178] provide a rich discussion on such issues, including on topography “versus” topology thinking in geography. By heeding the recent research on topologies published by geographers and social theorists, Bille[84] intends to contribute to the emerging mathematical turn. For historical, institutional economics and game-theoretic insights on Blockchain, see Berg[71] who studies similarities between two protocols – diplomacy in the Ancient Near East and blockchain.

Meanwhile, Blockchain Networks community structure analysis is being studied (see for example Chen[141] propose a “distributed community detection method”) and dynamic bitcoin transaction visualization patterns are provided (McGinn[386]).

While the Blockchain technology is spreading, combining such geographic, landscape research, historically oriented and network science analysis and tools would be deeply fruitful, especially with the emergence of smart cities.

### 3.6.2 Complex network analysis, transaction graph analysis, neutrosophic graphs


Miller et al.[397] analyze the measured topology to discover both high-degree nodes and a well connected giant component. Efficient propagation over the Bitcoin backbone does not necessarily result in a transaction being accepted into the block chain. They introduce a decloaking method to find influential nodes in the topology that are well connected to a mining pool. Their results find that in contrast to Bitcoin’s idealized vision of spreading mining responsibility to each node, mining pools are prevalent and hidden: roughly 2% of the (influential) nodes represented three quarters of the mining power. Javarone Wright[303] study the Bitcoin network and the Bitcoin Cash network, analyze their global structure and we try to evaluate if they are provided with a small-world behavior: their results suggest that the principle known as fittest-gets-richer, combined with a continuous increasing of connections, might constitute the mechanism leading these networks to reach their current structure. They provide further observations opening the way to new investigations into this direction. Yang Kim[602] examine a few complexity measures of the Bitcoin transaction flow networks and model the joint dynamic relationship between these complexity measures and Bitcoin market variables such as return and volatility. They find that a particular complexity measure of the Bitcoin transaction network flow is significantly correlated with the Bitcoin market return and volatility. More specifically we document that the residual diversity or freedom of Bitcoin network flow scaled by the total system throughput can significantly improve the predictability of Bitcoin market return and volatility.

Bovet et al.[102] by using the complete transaction history from December 5th 2011 to December 23rd 2013, this period including three bubbles experienced by the Bitcoin price and focus on the global and local structural properties of the user network (and their variation in relation to the different period of price surge and decline). Maesa et al.[372] analyse the topological properties of the Bitcoin transaction graph to obtain insights in the behaviour of the users, in particular outliers in the in-degree distribution of the bitcoin users graph, and argue that some users behaviors are not strictly related to normal economic interaction. Other analyses have been conducted for Bitcoin or for other networks (see [398, 406, 373, 140]). Maesa et al.[374] analyze the Bitcoin users graph and show by clustering the transaction graph, that the bow tie structure already observed for the graph of the web is augmented, in the Bitcoin users graph with the economical information about the entities involved, and perform a temporal analysis of the evolution of the resulting bow tie structure. Oggier et al.[431] generalize Tutzauer’ entropic centrality notion (that characterizes vertices which are important in the sense that there is a high uncertainty about the destination of an atomic flow
starting at them, assuming that at each hop, the flow is equally likely to continue to any unvisited vertex, or to be terminated there notion) to non-atomic flows and show using network graphs derived from Bitcoin transactions that depending on the graph characteristics, the presented entropy based centrality metric can provide a unique perspective not captured by other existing centrality measure, particularly in identifying vertices with relatively low out-degrees which may nevertheless be connected to hub vertices, and thus can have high spread in the network. For a survey on clustering, see Schaeffer[507]. Oggier et al.[432] propose one possible adaptation of the entropy measure Renyi quadratic entropy based measure in the context of graph clustering, exploring how the algorithm performs with subgraphs from the Bitcoin transactions network. Nagarajan[412] discuss on Blockchain single and interval valued neutrosophic graphs proposed and applied in transaction of Bitcoins, as well as degree, total degree, minimum and maximum degree for the proposed graphs, and give comparative analysis with advantages and limitations of different types of Blockchain graphs. Fadhil[205] provide some measurements briefly describing the Bitcoin networking aspects. Whang Chu Yang[577] about the details of mining pool behaviors (e.g., empty blocks, mining revenue and transaction collection strategies) and their effects on the Bitcoin end users (e.g., transaction fees, transaction delay and transaction acceptance rate). Chen[140] conduct a systematic study on Ethereum by leveraging graph analysis to characterize three major activities on Ethereum(money transfer, smart contract creation, and smart contract creation invocation). Fadhil et al. [443] introduce a proximity-aware extension to the current Bitcoin protocol, named Bitcoin Clustering Based Ping Time protocol (BCBPT). This protocol, that is based on how the clusters are formulated and the nodes define their membership, is to improve the transaction propagation delay in the Bitcoin network. Kieffer et al.[321] analyze Ethereums smart contract topology, finding high levels of contract activity (largely independent of price) but low levels of contract diversity: most contracts are direct- or near-copies of other contracts. Park et al.[452] present a comparative measurement study of nodes in the Bitcoin network. Forestier et al.[217] addresses the scalability issue by defining an architecture, called the blockclique, that addresses this limitation by sharding transactions in a block graph with multiple threads. See also [494, 518]. Rohrer et al.[494] provides a discussion on a topological based attack.

3.6.3 Fraudulous behaviors

Attacks. Detection. Tran[566] Stealthier Partitioning Attack against Bitcoin. Neudecker Hartenstein[422] provides a systematic approach that brings together known attacks, the requirements, and the design space of the network layer. Note that they include a summary of known network-based attacks on permissionless blockchains at the example of Bitcoin visualized as attack trees. Neudecker[421] provide also an empirical analysis of Blockchain forks in Bitcoin. Misic et al. 2019[402] for a recent paper on forks and fork characteristics in a Bitcoin-like distribution network. Note that Shalini[522] provide a survey on various attacks in Bitcoin and Cryptocurrency, see also Saad et al.[499] who explore the attack surface of the Blockchain technology and provide a systematic review. Javarone Wright[304] propose a model for double-spending detection for the Bitcoin network, the idea is detecting the presence of conflicting transactions by means of an ‘oracle’ that polls a subset of nodes of the Bitcoin network, assuming it to be a complex network. Phetsouvanh et al.[456] propose graph mining techniques to explore the relationships among wallet addresses (pseudonyms for Bitcoin users) suspected to be involved in a given extortion racket, exploiting the anonymity of the Bitcoin network to collect and launder money.

3.6.4 Evolving networks, dynamics


As studied in MarianneVerdier [572], the Blockchain obviously questions the power of intermedia-
aries on financial information. Decker Wattenhofer[171] early studied information propagation in the bitcoin network. For a reference point on information propagation in the Blockchain see Decker Wattenhofer[171]. Castells[127] on how information/network economy has transformed relationships, particularly social and economic relationships as well as reshaping the labor markets. Akcora 2018[8] model the Bitcoin network with a high fidelity graph (as Blockchain based crypto-currencies expose the entire transaction history to the public) so that it is possible to characterize how the flow of information in the network evolves over time and show this data representation permits a new form of microstructure modeling with the emphasis on the local topological network structure to study the role of users, entities and their interactions in formation and dynamics of crypto-currency investment risk, identifying certain sub-graphs (chainlets) that exhibit predictive influence on Bitcoin price and volatility and characterize the types of chainlets that signify extreme losses. Shhsavari et al.[521] present an analytical model using a random graph network and capture the Bitcoin network behavior and dynamics. Pappalardo et al.[450] investigate both the transaction dynamics and the block dynamics on the Bitcoin network, and find that the Bitcoin system fails in taking accurate record of the transactions with some of them taking months before being recorded in the Blockchain, although this inefficiency is much larger in terms of transaction recording than in terms of volumes exchanged. Fadhil[205] analyse how transaction validation is achieved by the transaction propagation round trip and how transaction dissemination throughout the network can lead to inconsistencies in the view of the current transactions ledger by different nodes. We then measure the transaction propagation delay in the real Bitcoin network and how it is affected by the number of nodes and network topology. This measurement enables a precise validation of any simulation model of the Bitcoin network. Large-scale measurements of the real Bitcoin network are performed. Bovet et al.[102] by using the complete transaction history from December 5th 2011 to December 23rd 2013, this period including three bubbles experienced by the Bitcoin price and beside focussing on the global and local structural properties of the user network and their variation in relation to the different period of price surge and decline. By analysing the temporal variation of the heterogeneity of the connectivity patterns they gain insights on the different mechanisms that take place during bubbles, and find that hubs (i.e., the most connected nodes) had a fundamental role in triggering the burst of the second bubble. Finally, we examine the local topological structures of interactions between users, we discover that the relative frequency of triadic interactions experiences a strong change before, during and after a bubble, and suggest that the importance of the hubs grows during the bubble. These results provide further evidence that the behaviour of the hubs during bubbles significantly increases the systemic risk of the Bitcoin network, and discuss the implications of public policy interventions. See Dixon et al.[179] transaction graph analysis and financial risk. Structure properties and anonymity of the bitcoin transaction graph have been studied (see Ober et al. [429]) See also Lischke Fabian[362], Baumann Fabian Lischke[58]. See Guo et al.[254] for a dynamic network perspective on the latent group structure of cryptocurrencies. Baçao et al.[41] investigates information transmission between cryptocurrencies. Chawla et al.[137] underline that improving how information is stored and more importantly, how it propagates across the (Blockchain) network, are open research questions and propose a block propagation approach while studying economic incentives and showing the benefits the proposed approach have to rational actors. Papadis et al.[449] develop stochastic network models to capture the Blockchain evolution and dynamics and analyze the impact of the block dissemination delay and hashing power of the member nodes on Blockchain performance in terms of the overall block generation rate and required computational power for launching a successful attack. Misic et al. 2019[402] investigate the performance of block propagation in a Bitcoin-like peer-to-peer distribution network and highlight the impact of the Nakamoto consensus protocol on the dynamics of blockchain growth. Li[359] markov processes in the queueing study of blockchain systems. Ben Van Lier (volume 1 chapter 5 in [189]) takes a wider perspective investigating the autonomy and self-organization of cyber-physical systems.
3.7 Multiplex networks, connecting blockchains and interoperability

3.7.1 Connecting blockchains, interledger, sidechains and cross-blockchain Technologies

Towards interoperability, see Buterin[111], Mattila[383] on the need of thinking on the scale of a network of systems. On the blockchain system and the cloud platform being interdependent see [368]. See also Robinson[492], Chitra[145]. Interledger encompasses several different approaches that attempt to establish interoperability among different distributed ledgers or blockchains. On Interledger see Thomas Schwartz[562] and Hope-Bailie Thomas[282] and refer to [533] for a recent survey. On sidechain see Back[42]. On the code diversity issue, see Reibel[484, 485]. These issues are linked with interoperability issues.

3.7.2 Interoperability

Hardjono et al.[263] for a recent discussion. Casino[125]: the growth of the number of cryptocurrency could raise interoperability problems due to the heterogeneity of cryptocurrency applications see Tschorsch and Scheuermann, 2016; Haferkorn and Quintana Diaz, 2015) see Casino[125] section on Blockchain adoption and interoperability. Interoperability between Blockchains as well as between Blockchains and other technologies are clearly crucial issues and paths to solutions are ongoing.16

Clearly Multiplex networks analysis and methods (see Boccaletti[92], Bianconi[80], Battiston et al.[57]) are to provide frameworks for Blockchain analysis and methods. How about for instance the description in Chakraborty[133]? For competition among networks, one can see for example Iranzo[300] and Fan[207] on game theory between networks. Note that Lee[348] develops a game theory Nash equilibrium model for IoT. Some blockchains involve studying networks with (even temporary) heterogeneous nodes, such as (maybe temporary) leading nodes, validating nodes (see for instance Belotti et al.[65]).

3.8 Economic analysis, networks and Blockchains: some insights towards new frameworks and models?


Mainly, the development of Blockchain ecosystems leads both to adapt existing frameworks and models and to depart from them. Clearly economic analysis and network science are to be more more crucially intertwined (see Garcia et al.[224]). See Swan editor[549] and early overviews and introductions (see Catalini Gans[129] Davidson et al.[165]17, Abadi Brunnermeier[1]). Caliskan[117] question the framework of economic and social models analysis adapted to Blockchain development. Pagnotta Buraschi[447] consider a new type of production economy “a decentralized financial network (DN)”. They formalize such a Decentralized Networks economy and address the valuation of bitcoins and other blockchain tokens. An identifying property of these assets is that contributors to the DN trust (miners) receive units of the same asset used by consumers of DN services, and then the overall production (hashrate) and the bitcoin price are jointly determined. They characterize the demand

16See Koens[331], Schulte[512], Koen[329], Hardjono[262], Brogan[104], Pillai[459], Krishnan[335], [262], [483].
17Davidson De Filippi Potts[165] provides some propositions for building analytical frameworks for economics of blockchain (suggests two approaches to economics of blockchain: innovation-centred and governance-centred. Argues that the governance approach based in new institutional economics and public choice economics is most promising, because it models blockchain as a new technology for creating spontaneous organizations, i.e. new types of economies).
for bitcoins and the supply of hashrate, show that the equilibrium price is obtained by solving a
fixed-point problem and study its determinants. Meunier[393] discusses Bitcoin, Distributed Ledgers
and the Theory of the Firm. How about General equilibrium? (see empirical study Aoyagi 2019[31]
and He[269] constructing a general equilibrium model of PoW protocol based blockchain network).
As we have already seen, Institutional economics is clearly greatly concerned (Berg et al.[74, 69]).
Allen et al.[13] analyze democracy as an economic problem of choice constrained by transaction
costs and information costs. Society must choose between competing institutional frameworks for
the conduct of voting and elections, these decisions being constrained by the technologies and insti-
tutions available. As Blockchains are a governance technology, it could be applied to the voting
and electoral process to form a crypto-democracy. Analysed through the Institutional Possibility Frontier
framework, they propose that blockchain lowers disorder and dictatorship costs of the voting and
electoral process (Allen et al.[13]). How about Public choice? (Oguro[433], Berg[70]), taxation issues
(Houben et al.[284], Ahmad[7]). On Auditing, see Abreu[5], Pienmetl 2019[460] and the report[81].
On how generally (i.e. not specifically by blockchains) smart connected products are transforming
competition, see Porter[467]. On how generally (i.e. not specifically by blockchains) Breidbach[103]
technology is transforming the role of the firm. Pilkington[458] while analyzing Bitcoin through the
lenses of complexity theory, argue that rationality, equilibrium and self-interest, the Bitcoin phe-
omenon would cast light on the emergence of non-intuitive macroeconomic results derived from
numerous micro-interactions involving groundbreaking technology, and argues how knowledge fields,
such as monetary policy and banking regulation have been shaken by Bitcoin, while articulating
a reflection on the new geography of money and finance. How about Game theory? (see Biais et
al.[79] on the Blockchain folk theorem, mean-field game theory in Barreiro et al.[53], [39] for SoK-
tools for game theoretic models of security for cryptocurrencies, Amoussou et al.[22] modelize the
Byzantine-consensus based blockchains as a committee coordination game, Wang Tang[582] for a
game-theoretic analysis of pool strategies selection in PoW-based Blockchain Networks, Jaag[61] on
the bitcoin mining game, Liu[366] for a recent survey on applications of game theory in Blockchain,
etc).

3.9 CRYPTOCURRENCY AND BANKING

3.9.1 Money

Money and programmable money. Is Bitcoin a Money?
See Elsden 2019[198] on programmable money. See also Kubat 2015[336] ,Ammous[21], Dai Sidiro-
poulos and al.[158]. Guegan[248] argues Bitcoin is not a currency from a monetary point of view.
“The circulation of Bitcoin is slow and quantity is limited, so from an economical point of view, Bit-
coin is not adapted to the demand for money, cannot help to revive the economy (credit), nor to
control inflation. In the case of the purchase of a property, the transactions cannot be canceled, even
if the property is not delivered. It can make the exchanges difficult. One can encounter difficulty in
converting Bitcoins into Euros (for instance) (no guarantee of convertibility of the currency by the
public authorities). The circulation speed is low: only 4% of the bitcoins in circulation are weekly
used. This is more like a casino economy, and since there is currently no regulation, no central bank
ensures the stability of the value”. Milkau Bott[396] discuss on Digital currencies and the concept of
money as a social agreement. Grym[245] argue cryptocurrencies are not money.
See also Guegan[249]. Kuikka[338] discusses if cryptocurrency can come to fulfill the functions of
money and evaluates cryptocurrency as a global currency.

3.9.2 Currency pluralism, Central bank digital currency, Currency competition

banking.
Seang Torre[513] examines in a theoretical setting the properties of two Blockchain consensus protocols (Proof of Work (PoW) and Proof of Stake (PoS)) in the management of a local (or networks of local) complementary currencies. See also Adrian et al. 2019[6] the rise of digital money. Lutz[369] on Currency Competition. For a recent paper on central bank digital currency see Belke et al.[63]. Belke et al.[63] discusses the main questions to the ongoing debate on central banking and cryptocurrencies: major characteristics of today’s payments systems, pros and cons of still having (partially) tangible means of payment, might cryptocurrencies (and underlying blockchain technology) might somehow contribute to establishing a more modern, secure and stable payments system, etc. Arjalies[32] on alternative finance. see Glaser[234] for a link between blockchain and free banking. See also Hayek[575], see White[587] Williamson[589] discusses the welfare and policy implications of Central Bank Digital Currency. See also Berg[74].

3.10 Markets

3.10.1 Impact on markets


See Zamani[607] on distributed ledger technology and market disintermediation. On personal data markets, one can refer to Spiekermann 2015[540]. On the GDPR and data markets Politou 2018[465] “While the principles encompassed by the GDPR were mostly welcomed, two of them, namely the right to withdraw consent and the right to be forgotten, caused prolonged controversy among privacy scholars, human rights advocates and business world due to their pivotal impact on the way personal data would be handled under the new legal provisions and the drastic consequences of enforcing these new requirements in the era of big data and internet of things. In this work, we firstly review all controversies around the new stringent definitions of consent revocation and the right to be forgotten in reference to their implementation impact on privacy and personal data protection, and secondly, we evaluate existing methods, architectures and state-of-the-art technologies in terms of fulfilling the technical practicalities for the implementation and effective integration of the new requirements into current computing infrastructures. The latter allow us to argue that such enforcement is indeed feasible provided that implementation guidelines and low-level business specifications are put in place in a clear and cross-platform manner in order to cater for all possible exceptions and complexities.” Molina et al. 2019[404] develop a decentralized conceptual marketplace model for IoT generated personal data, thinking personal data as a marketplace product and a marketplace model in which such a product could be effectively bought and sold without compromising the privacy of the data subject. Foy 2019[218] provides a financial accounting classification of cryptocurrency. See also Melse 2018[388], Karajovic 2019[314].

3.10.2 Financial risk, cryptocurrency markets

Can the transaction graph analysis provide warning insights on financial losses? how can Blockchain Economic Network theory contribute to the analysis of systemic risk? what about the study of cryptocurrency markets? how to conduct portfolio analysis and asset pricing?

Swan (volume 1 chapter 1 in [189]) develops insights on Blockchain Economic Network theory and discusses how the widespread adoption of blockchain technology might contribute to solving a larger class of economic problems related to systemic risk. For a broad recent discussion on this issue, see Swan[548]. Refer also to Battiston Caldarelli[56]. Dixon et al.[179] ask in which extent the transaction graph can serve as an early-warning indicator for large financial losses and demonstrate the impact of extreme transaction graph activity on the intraday volatility of the Bitcoin prices series. Specifically, they identify certain sub-graphs (‘chainlets’) that exhibit predictive influence on Bitcoin price and volatility and characterize the types of chainlets that signify extreme losses. Using bars ranging from 15 minutes up to a day, they fit GARCH models with and without the extreme chainlets.

3.11 Law

For a survey on Blockchain issues and the law, we refer to Filippi Wright[169] and Berg et al.[69], see also Ostbye[441] on liability issue if a public cryptocurrency protocol fails. De Filippi Wright[593] on the widespread deployment of Blockchains will lead to expansion of a new subset of law, which they term Lex Cryptographia. See also McCallum[385] and Bolotaeva[94], Lessig[353, 354], Wu[594] and link between blockchain and lessig see Filippi Hassan[169], De Filippi[169]. On regulating Blockchain and Cryptocurrencies, see also Shanaev et al.[523], Hazar[267]. Scholl Bolivar[511] analyse the case of Gibraltar not only as the first jurisdiction worldwide to regulate general DLT provision, but as well as using the regulation as a competitive tool and a means for creating new public value. Nabilou[410, 411]. See Johansson 2019[307] on RegTechs. On GDPR and Blockchains, Truong 2019[568] propose a Blockchain-based Solution for GDPR-Compliant Personal Data Management. On the right to withdraw consent and the right to be forgotten, see Politou 2018[465]. There are many discussion papers on Blockchain technology and the gdpr, see Berberich 2016[68], Salmensuu 2018[503]. Buocz 2019[108] on Bitcoin, gdpr and allocating responsibility in distributed networks See Magnier[375] on the potential impact of Blockchains on corporate governance: a survey on shareholders' rights in the digital era, for a literature review on use of Blockchain in governance Razzaq[482], see also Davidson et al.[164], De Filippi Hassan[266].

4. Beyond

4.1 Risks

Numerous risks and challenges have been mentioned throughout the previous sections. It is crucial to take into account each of but also the interplay dynamics/intertwined risks of the human element, information systems, and communication networks.

There are many definitions and conceptions of risks, and this issue (Blockchain and Cryptocurrency) is clearly deeply multi-faceted, and clearly all domains are concerned there. We give some of the related issues. For example, houy[285] argues that killing a proof of stake can be done at no cost.

18Note that Girasa has also written more generally on Cyberlaw. Refer to Girasa[231]
The storage and obsolescence (obsolescence of platform implementations) can also be an issues. Østbye[439] “As the role of cryptocurrencies in the economy increases, such model risk is likely to be a concern for regulators. The regulatory implications of model risk are also discussed in this paper.” See also Østbye[440]. Matzutt et al.[384] provide a systematic analysis of the benefits and threats of arbitrary blockchain content, as blockchains irrevocably recording arbitrary data which does not come without risk for users as each participant has to locally replicate the complete blockchain, particularly including potentially harmful content. See Zetzsche[609] on legal risks of blockchains. Bielinsky Soloviev[82] on indicators based on complex network structure. Soloviev[536] Methods of nonlinear dynamics and the construction of cryptocurrency crisis phenomena precursors. See Chia[143] on cascading failures in blockchains. Goldfeder et al.[237] on cookie and the blockchain, and ODair [430] on risks of adoption.

4.2 Adoption, digital divide, digital culture and education


Swan[547] notes that the term digital divide has typically referred to the gap between those who have access to certain technologies and those who do not. Hooks[281] discusses on how Blockchain and alternative networks can bridge the digital divide and facilitate economic inclusion. Parino et al.[451] propose to characterize the adoption of the Bitcoin blockchain by country, underlying the fact that while the Bitcoin blockchain attracts a lot of attention, it remains difficult to investigate where this attention comes from, due to the pseudo-anonymity of the system, and consequently to appreciate its social impact. As emphasized in Abraham[3], numerous factors play roles in influencing Bitcoin penetration and acceptance, both at country and individual level, such as trust, perceived risk, security threat, perceived benefit, perceived ease of use, as well as macrotechnological and socioeconomic factors. Stix 2019[544] finds that among Austrian households, ownership and purchase intention of crypto-assets are strongly affected by profit expectations and by beliefs that crypto-assets offer advantages for payments -most adopters or potential adopters hold both beliefs. Perceptions of high volatility or the risk of fraud and online theft dampen the demand for crypto-assets. Presthus 2017[470] provide an analysis of motivations and barriers for end-user adoption of bitcoin as digital currency. Mendoza 2018[389] study social commerce as a driver to enhance trust and intention to use cryptocurrencies for electronic payments. Studies through network analysis deep tools on adoption and diffusion of blockchain and cryptocurrency related assets are to be conducted (see for example [610]).

Cai 2019[116] provide evidence that network structure can trigger smart contract adoption (focusing on CryptoKitties adoption in the Ethereum network). Many have conscious of this. As Judmayer et al. (volume 2 in [189]) “Bitcoin show how difficult the fundamentals are to understand for nonexpert users, not to mention the fact that there is still very little awareness or understanding of systems other than cryptocurrencies that rely on the principle of blockchains.”, which their Appendix on Blockchain basics contributes helping understanding of the underlying concepts, presenting the basic ideas behind Bitcoins complex components in a way that makes it easy to understand without technological knowledge through using an example of a stone block chain that uses simple analogies that are easy to visualize. See also initiatives as the five volumes comic Las Aventuras de Quirquincho by Castro and Quezada[128], Quirquincho going through diverse adventures that explain basic concepts of the Blockchain. Even if, for usages, knowing the technical very aspects of Blockchain is not needed, digital culture has to be spread, including some basis in Network science tools, as understanding literature and texts wouldn’t need to master the technical very aspects of printing but tools developed and needed to understand and read texts with deeper acuity. Wing[590, 591] argue that to reading, writing, and arithmetic, we should add computational thinking to every child’s analytical ability. See also Atlan et al.[37], Lu[367], Grover[241], Yadav[600], Barr[51, 52], Hambrusch[261], Henderson[272].
4.3 Quantum computing and Blockchain, Quantum Blockchains, Quantum Networks

See Kiktenko et al.[322]: current blockchain platforms rely on digital signatures, which are vulnerable to attacks by means of quantum computers. Kiktenko et al.[322] propose a possible solution to the quantum-era blockchain challenge and report an experimental realization of a quantum-safe blockchain platform that utilizes quantum key distribution across an urban fiber network for information-theoretically secure authentication. See also Fedorov[209], Rodenburg[493], Stewart[542], Ikeda[298], Sattath[506], Gao[221], Jogenfors[306], Yin[604]. On Quantum money see Rajan[474], Ingber[299], Ikeda[297], Horodecki[283], Ablayev[2], Sun[546], Sun[545] (voting protocol), Li[355] (post-quantum blockchain networks), Bennet Daryanoosh[66], see also Casino[125] on quantum resilience.

4.4 Sustainability and energy consumption

Refer to Casino[125] on sustainability of the blockchain protocol.

Marcus Dapp (volume 2 chapter 6 in[189]) argue for a new economic approach that has sustainability built into its core design by using cryptoeconomics based on blockchain technology to create incentive systems which encourage sustainable behavior.

Leonard Treiblmaier (volume 2 chapter 7 in [189]) question the economic growth paradigm and ask the question whether cryptocurrencies can help to create a more sustainable economy. See also Alvarez-Pereira[19]. For example, alternatives are being looked for (see Amoussou-Guenou[23]).

5. Conclusion


There are many issue-related categorizations, being refined and more and more accurate. However, towards the technical characteristics, specificities and impacts that are particular to the development of Blockchains, the need for building more general frameworks for Blockchain related-issues analysis may arise. As Judmayer et al. (volume 2 chapter 15 in [189]) argue many unsolved problems in terms of finding a balance between performance, scalability, security, decentralization, and anonymity in such systems. Casino[125] also emphasizes those issues: “All these approaches imply some additional changes in the balance between security, scalability, and decentralisation that blockchains offer by default. Therefore, considerable research effort needs to be undertaken for finding the proper equilibrium”. Such balances are to be dealt also through categorizations as provided in Kannengiesser et al.[313]. As well as other disruptive technologies but also from their specificities, Blockchain and cryptocurrencies’ technologies is also an opportunity for researchers from any areas to reflect on such a disruptive innovation, both from its impact and development observation. It’s a good example to study innovation adoption, including observing the anticipating analyses from a multileveled viewpoint. As Cardon[122] emphasizes, it is important to have various and interdisciplinary knowledge for living there with agility and prudently, as if we make the digital, the digital also makes us. As digital disruption can be deeply compared with Printing disruption, and we know that it has had many consequences on thinking, religion, organizational power etc (see Eisenstein[193, 194, 195, 50]), the ongoing Blockchain revolution being part of the digital disruption, it is crucial to develop tools from various and interdisciplinary research for attempts to capture it. What will be the consequences and how will we face them? While Xu et al.[598] argue that “to achieve the benefits touted from

---

19(our translation from French) Cardon: “Il est important de disposer de connaissances variées et interdisciplinaires pour y vivre avec agilité et prudence, car si nous fabriquons le numérique, le numérique nous fabrique aussi”([122])
blockchain will require a degree of cooperation among institutions that has not yet been achieved
and that could have been achieved with modifications of existing technology”, Blamont[88] proposes
to think about a structure called “Fédération” consisting in establishing a functional link between
collaborative communities and established hierarchies, between “exuberance of the crowd” and “rigor
of the norm” and Swan underlines that “there is a need for a decentralized ecosystem surrounding
the blockchain itself for full-solution operations” ([547], p.19). While transdisciplinary surveys are
provided on Blockchain, it becomes clearer and clearer how Network Science can provide tools and
analysis making fruitful interdisciplinary researches flourish. It is crucial to take into account each of
but also the interplay dynamics/intertwinned analysis of the human elements, information systems,
and communication networks.

REFERENCES

uary 5th version.


and penetration of bitcoin: The role of psychological distance and national culture. SAGE


[5] Pedro W Abreu, Manuela Aparicio, and Carlos J Costa. Blockchain technology in the audit-
ing environment. In 2018 13th Iberian Conference on Information Systems and Technologies
(CISTI), pages 1–6. IEEE, 2018.

Monetary Fund, 2019.

[7] Ashar Ahmad, Muhammad Saad, and Aziz Mohaisen. Secure and transparent audit logs with


[10] Maher Alharby and Aad van Moorsel. Blockchain-based smart contracts: A systematic map-


[12] Darcy WE Allen, Alastair Berg, and Brendan Markey-Towler. Blockchain and supply chains:
V-form organisations, value redistributions, de-commoditisation and quality proxies. Value
Redistributions, De-Commoditisation and Quality Proxies (December 12, 2018), 2018.


[33] Arie Arnon. Free and not so free banking theories among the classicals; or, classical forerunners of free banking and why they have been neglected. *History of political economy*, 31(1):79–107, 1999.


Gregory Benson Jr. Implications of adopting blockchain technology on international sales transactions. 2019.


Chris Berg. What diplomacy in the ancient near east can tell us about blockchain technology. Ledger, 2017.


Xudong Cai, Xi Zhao, Bin Zhang, and Gengzhong Feng. Identifying multiple peer influences on smart contract adoption in blockchain user network. *Available at SSRN 3387794*, 2019.


Sinclair Davidson, Primavera De Filippi, and Jason Potts. Disrupting governance: The new institutional economics of distributed ledger technology. 2016.

Sinclair Davidson, Primavera De Filippi, and Jason Potts. Economics of blockchain. 2016.


Primavera De Filippi and Xavier Lavayssière. Blockchain technology: toward a decentralized governance of digital platforms?


Primavera De Filippi and Xavier Lavayssière. Blockchain technology: toward a decentralized governance of digital platforms?


[190] Christopher Ehmke, Florian Blum, and Volker Gruhn. Properties of decentralized consensus technology–why not every blockchain is a blockchain.


[239] Mr Tommaso Mancini Griffoli, Mr Maria Soledad Martinez Peria, Mr Itai Agur, Mr Anil Ari, Mr John Kiff, Ms Adina Popescu, and Ms Celine Rochon. *Casting Light on Central Bank Digital Currencies*. International Monetary Fund, 2018.


[251] Rachid Guerraoui. Si la blockchain est la solution, quel est le problème ? (in french, if the blockchain is the solution, what is the problem?). *available at https://www.college-de-france.fr/site/rachid-guerraoui/course-2019-03-01-10h00.htm*, 2018.


[266] Samer Hassan and Primavera De Filippi. The expansion of algorithmic governance: From code is law to law is code. Field Actions Science Reports. The journal of field actions, (Special Issue 17):88–90, 2017.


[277] Janine Hobeika and Chee Yoong Liew. Is bitcoin under influence?


[301] Zsolt István. Something new under the sun: Thoughts on optimizing the performance of blockchains.


Rose Mahdavieh. Governments’ adoption of native cryptocurrency: A case study of Iran, Russia, and Venezuela. 2019.


Julio Mendoza, Higinio Mora, Francisco A Pujol, and Miltiadis D Lytras. Social commerce as a driver to enhance trust and intention to use cryptocurrencies for electronic payments. 2018.


[414] Voraprapa Nakavachara, Tanapong Potipiti, and Thanawan Lertmongkolnam. Should all blockchain-based digital assets be classified under the same asset class? *Available at SSRN 3437279*, 2019.


[428] Juha Nokelainen. Analysing the effects of general data protection regulation article 17 on blockchain technology.


[441] Peder Østbye. Who is liable if a public cryptocurrency protocol fails? Available at SSRN 3423681, 2019.


[448] K Palanivel. Blockchain architecture to higher education systems.


Mohamad Saleh. Cryptonomics: Investment behaviour in the cryptocurrency market.


Stefan Schulte, Marten Sigwart, Philipp Frauenthaler, and Michael Borkowski. Towards blockchain interoperability.


attack against bitcoin peer-to-peer network.


[568] Nguyen Binh Truong, Kai Sun, Gyu Myoung Lee, and Yike Guo. Gdpr-compliant personal

[569] Florian Tschorsch and Björn Scheuermann. Bitcoin and beyond: A technical survey on de-
centralized digital currencies. IEEE Communications Surveys & Tutorials, 18(3):2084–2123,
2016.


[571] Selinde van Engelenburg, Marijn Janssen, and Bram Klievink. A blockchain architecture for
reducing the bullwhip effect. In International Symposium on Business Modeling and Software

[572] Marianne Verdier. La blockchain et l’intermédiation financière. Revue d’économie financière,

[573] Wattana Viriyasitavat and Danupol Hoonsopon. Blockchain characteristics and consensus in

[574] Galyna Volokhova and Anastasiia Volokhova. Corporate identity of blockchain-based compan-
ies. Sustainable development under the conditions of European integration. Part II, page 448,
2019.

Institute, 2009.

[576] Nick Vyas, Aljosja Beije, and Bhaskar Krishnamachari. Blockchain and the Supply Chain:

[577] Canhui Wang, Xiaowen Chu, and Qin Yang. Measurement and analysis of the bitcoin networks:

[578] Jingzhong Wang, Mengru Li, Yunnhua He, Hong Li, Ke Xiao, and Chao Wang. A blockchain
based privacy-preserving incentive mechanism in crowdsensing applications. IEEE Access,

A summary of research on blockchain in the field of intellectual property. Procedia computer

[580] Licheng Wang, Xiaoying Shen, Jing Li, Jun Shao, and Yixian Yang. Cryptographic primitives

[581] Wenbo Wang, Dinh Thai Hoang, Peizhao Hu, Zehui Xiong, Dusit Niyato, Ping Wang, Yonggang
Wen, and Dong In Kim. A survey on consensus mechanisms and mining strategy management

selection in pow-based blockchain networks: Game-theoretic analysis. IEEE Access, 7:8427–
8436, 2019.


Steve Y Yang and Jinhyoung Kim. Bitcoin market return and volatility forecasting using trans-
action network flow properties. In 2015 IEEE Symposium Series on Computational Intelligence,

Wenli Yang, Erfan Aghasian, Saurabh Garg, David Herbert, Leandro Disiuta, and Byeong Kang. A survey on blockchain-based internet service architecture: Requirements, challenges,

Wei Yin, Qiaoyan Wen, Wenmin Li, Hua Zhang, and Zhengping Jin. An anti-quantum trans-

Steve Young. Changing governance models by applying blockchain computing. Catholic Uni-

Haifeng Yu, Ivica Nikolic, Ruomu Hou, and Prateek Saxena. Ohie: Blockchain scaling made

Efpraxia D Zamani and George M Giaglis. With a little help from the miners: distributed ledger technology and market disintermediation. Industrial Management & Data Systems,

Alexei Zamyatin, Katinka Wolter, Sam Werner, Peter G Harrison, Catherine EA Mulligan, and


JingMing Zhang, ShuZhen Zhu, Wei Yan, and ZhiPeng Li. The construction and simulation of internet financial product diffusion model based on complex network and consumer decision-


Ren Zhang and Bart Preneel. Lay down the common metrics: Evaluating proof-of-work cons-
ensus protocols? security. In 2019 IEEE Symposium on Security and Privacy (SP). IEEE,
2019.


