Article:
Febrero, P and Pereira, J orcid.org/0000-0001-9268-9842 (2022) Cryptocurrency Constellations across the Three-Dimensional Space: Governance Decentralization, Security, and Scalability. IEEE Transactions on Engineering Management, 69 (6). pp. 3127-3138. ISSN 0018-9391

https://doi.org/10.1109/TEM.2020.3030105

Cryptocurrency Constellations across the Three-Dimensional Space: Governance Decentralization, Security, and Scalability

Pedro Febrero

Bityond, Cryptoners
Lisbon, 1600-402 Portugal
Email: pedro.febrero@bityond.com

Joana Pereira

Leeds University Business School, University of Leeds
Leeds, LS2 9JT UK
Email: j.pereira@leeds.ac.uk

ABSTRACT

In the post-Bitcoin era, many cryptocurrencies with a variety of goals and purposes have emerged in the digital arena. This paper aims to map cryptocurrency protocols across governance decentralization, security, and scalability, theorizing about the organizational and technological features that impact these dimensions. Such organizational and technology protocol features encompass roles permissiveness, validation network size, resource expenditure, and TPS (transaction per second). Based on these dimensions, we map the different cryptocurrency constellations based on their consensus mechanisms, illustrating how the various protocols applications experience and play with trade-offs among governance decentralization, security, and scalability.

***Index Terms*—Cryptocurrency protocols, blockchain technology, decentralized governance, scalability, security.**

I. INTRODUCTION

Despite the hype around blockchain technology, the central attempts to understand relate to the technical aspects of the technology and its potential applications in the financial sector, as with the case of Bitcoin (Risius and Spohrer, 2017). However, as the technology evolved, a variety of distinct cryptocurrency protocols were born, sprouting new narratives and use-cases to the blockchain technology. In fact, since the creation of the cryptocurrency Bitcoin protocol in 2008/2009, thousands of other cryptocurrencies have emerged (Evans, 2014; Corbet et al., 2019) in the areas of micropayments, storage systems, intellectual property, financial and physical assets, supply chain and logistics, social networks, media, and open science, among other applications (Davidson, De Filippi, and Potts, 2018; Li et al., 2017).

While new definitions, theoretical framings, and empirical evidence continue to grow, there is a strong need to distinguish between cryptocurrency protocols, their core technologies, currencies, and also what are the central distinguishing vectors among one another. This paper is, thus, an attempt to investigate theoretically such dimensions, proposing a systematic approach, which can explain why some cryptocurrency protocols are more decentralized, secure, or scalable than others.

In the early days of Bitcoin, there was not much distinction between Bitcoin, the cryptocurrency protocol, and blockchain, the block-based timestamped distributed ledger that sustains Bitcoin—the Bitcoin database (Fani et al., 2019; Nakamoto, 2008). Indeed, the terms blockchain and cryptocurrency are still misused nowadays. However, in this paper, we make the distinction between cryptocurrency protocols and data infrastructure, arguing that the blockchain is only one type of distributed ledger infrastructure. While blockchain is widely adopted by most of the cryptocurrency protocols, it is not the only database structure, nor the sole attribute of cryptocurrency protocols. On the top of distributed ledger, cryptocurrency

protocols display other distinguishing components as cryptography, cryptocurrency incentives, and a distributed consensus mechanism.

The intersection of these different technology components not only makes cryptocurrency protocols different from other existing protocols and currencies, such as digital, cryptographic, or even fiat currencies, but also allows cryptocurrencies to achieve inclusion, availability, divisibility, integrity, transparency, confidentiality, authenticity, and accountability (Biswas and Muthukkumarasamy, 2017; Corbet et al., 2019; Vigna and Casey 2015). In this paper, we define a cryptocurrency protocol as a system fueled by cryptocurrency incentives that allow nodes to transact in a peer-to-peer (P2P) network, following a particular consensus mechanism to reach agreement on the state of every cryptographically secured transaction of the distributed ledger (Catalini and Gans, 2017; Corbet et al., 2019; Davidson et al., 2018; Nakamoto, 2008; Pereira, Tavalaei, and Ozalp, 2019).

Researchers and practitioners have discussed the specific dimensions of the protocols in distributed computing and blockchain, as is the case of Brewer's CAP theorem (consistency, availability, and partition tolerance) on distributed computing, and Ethereum's trilemma on blockchain (decentralization, security, and scalability). This paper adds to the literature on cryptocurrencies by investigating the trilemma dimensions systematically, explaining how organizational and technological features, such as roles permissiveness, validation network size, resource expenditure, and TPS (transactions per second) affect governance decentralization, security, scalability, and inherent trade-offs.

In the following sections of the paper, we discuss what a cryptocurrency protocol is and expand on its technological components. Afterwards, we detail the three dimensions—governance decentralization, security, and scalability—and their respective features, suggesting some propositions for future research. Finally, we map the cryptocurrency constellations around the different consensus mechanisms and individual variations,

illustrating with examples, and we discuss the limitations of this study and suggestions for future research.

II. CRYPTOCURRENCY PROTOCOLS

Protocols are the rules, or the accepted standards, that define what an application can and cannot do within a set environment. Some widely known examples of protocols are HyperText Transfer Protocol (HTTP), which websites such as YouTube and Facebook obey, or Simple Mail Transfer Protocol (SMTP) and Post Office Protocol (POP3), used for the emails we exchange every day (see Liquid, 2018). As with these examples, cryptocurrencies also run over protocols that define the rules and standards of transactions. To a certain extent, cryptocurrency protocols obey a logic that is remarkably similar to that of previous internet protocols, like IPv4, IPv6, and HTTP, mainly in terms of their structure. Much like internet protocols, cryptocurrencies have a physical layer, a communication layer, and an interface layer (Biswas and Muthukkumarasamy, 2017). Therefore, each cryptocurrency project has its protocol, like Bitcoin, Ethereum, amongst others (Liquid, 2018).

However, while cryptocurrency protocols share the same structure as other existing protocols, the technology of cryptocurrencies are fundamentally different, as cryptocurrency protocols emerge at the intersection of four various technological components, specifically cryptography, distributed ledgers, cryptocurrency incentives, and consensus mechanisms. While each of these components exists in other protocols and applications in isolation, cryptocurrency protocols present these four components simultaneously, which makes them different from other existing protocols, such as digital, cryptographic, or even fiat currencies.

Cryptocurrency protocols use cryptography technology, which allows the sending of secure messages between two participants (P2P), where the sender sends an encrypted message, and the receiver needs to decrypt it to access the original message (Dinh et al., 2018). Additionally, these protocols also use PGP, or "pretty-good-privacy," encryption, which creates private-

public addresses, allowing any user to prove that they are the owner of a piece of data without showing their master key (or password). Cryptocurrency protocols use both cryptography and antispam technologies to perform secure, anonymous (or pseudo-anonymous), and immutable transactions. Such technologies also contribute toward quick, efficient, and cost-effective auditing processes, and protection against double-spending (Dinh et al., 2018).

Another core characteristic of cryptocurrency protocols is distributed ledger technology (DLT), that is a distributed data infrastructure where the posting of transactions writes data on the ledger (Dinh et al., 2018). Cryptocurrency protocols' ledger of transactions, which records the history of all trades, is stored in many locations simultaneously in a distributed manner (Nakamoto, 2008). The distributed ledger reinforces immutability, efficient auditing of transactions, and improved tamper-proofing and reliability. There are some variants of distributed ledgers. The most famous is, of course, blockchain, which structures the data in timestamped blocks linked through a cryptographic hash (Fani et al., 2019). However, there are also other DLTs used in cryptocurrency protocols, such as Directed Acyclic Graphs (DAGs), or HashTree.

Cryptocurrency protocols also integrate consensus mechanisms (Dinh et al., 2018), deeply connected to the distributed ledger. A consensus mechanism dictates the rules that validators and users must follow to participate in a network, building agreement among a network of mutually trustless participants. In essence, consensus mechanisms encompass the rules on how to add transactions to the ledger, allowing cryptocurrency protocols to run without the need for a trusted intermediary, as the consensus mechanism makes nodes agree on transaction data, such as amount, addresses, and accounts. The consensus mechanism is among the most defining dimensions of the cryptocurrency protocols, as it defines and interacts with the other cryptocurrency protocol components, such as cryptography, the distributed ledger, and cryptocurrency incentives. The most widely known consensus mechanisms are Proof-of-Work

(PoW), Proof-of-Stake (PoS), and Delegated Byzantine Fault Tolerance (DBFT) (Wang et al., 2020).

The last but no less critical defining characteristic of cryptocurrency protocols is the cryptocurrency incentives. Cryptocurrency incentives are fungible and tradable assets exchangeable within the platform to buy complements or convert into other cryptocurrencies or fiat currencies (such as USD or EUR) outside the focal venue. Cryptocurrency incentive schemes provide a reward to people providing labour, computing power, or other resources when recording and verifying transactions, or even voting on governance (Evans, 2014). The cryptocurrency incentives schemes serve to attract participants to register, validate, vote, or even perform transactions, fostering a decentralized coordination among participants. In other words, cryptocurrency incentive systems elicit efforts from a distributed global workforce to verify and record transactions on the ledger without the need for a central authority to control and validate transactions (Evans, 2014).

In short, a cryptocurrency protocol is a system fueled by cryptocurrency incentives that allow nodes to transact in a peer-to-peer (P2P) network, following a particular consensus mechanism to reach agreement on the state of every cryptographically secured transaction of the distributed ledger (Catalini and Gans, 2017; Corbet et al., 2019; Davidson et al., 2018; Nakamoto, 2008; Pereira et al., 2019) (see Table I).

TABLE I
CRYPTOCURRENCY PROTOCOLS' DISTINGUISHING COMPONENTS

Components	**Network Objectives**	**Supporting technology**
Cryptography	Security; anonymity (or pseudo-anonymity); immutability; auditing process	Public key cryptography, PGP, hashing
Distributed ledger	Immutability, auditability, tamperproof, and reliability	Blockchain technology, HashTree, Directed Acyclic Graphs (DAGs)
Consensus mechanisms	Consistency, liveliness, fault tolerance, protection against double-spending	PoW, PoS, DBFT, among others.
Cryptocurrency incentives	Participation, coordination, decentralization	Tokens, cryptocurrencies

III. KEY DIMENSIONS OF CRYPTOCURRENCY PROTOCOLS

Around 30 years ago, Eric Brewer introduced the CAP theorem of distributed computing. Such theorem states that network shared data-systems can only provide simultaneously two out of the following three dimensions: consistency (the ability of servers to return the right response to each request), availability (the degree to which each request receives a response), and partition tolerance (the ability of the servers to perform even considering delayed and lost messages between servers) (Brewer, 2000). Recently, the Ethereum team adapted such theorem in light of blockchain protocols, arguing that blockchain-based protocols can only deliver two of the trilemma's dimensions: governance decentralization (degree of transactions disintermediation) (Bohme et al., 2015; Davidson et al., 2018), security (network resilience, fault-tolerance, and immutability when facing attacks), and/or scalability (ability to handle a growing number of transactions) (Ethereum, 2019; see also Cholan, 2019; Fani et al., 2019; Manoppo, 2018). We build on the Ethereum's scalability trilemma, conceptualizing these dimensions as continuous, such that a cryptocurrency protocol could potentially be at any point along each dimension. Also, we theorize on the organizational and technological features that influence each extent. For the sake of brevity, in our propositions, we focus on the five main features of the cryptocurrency protocols: roles permissiveness, validation network size,

resource expenditure, and TPS (transactions per second). We ignore other technology dimensions such as communications protocols (Whisper), oracles, like Chainlink and peer-to-peer version-controlled file system, also known as decentralized storage protocols (IPFS) (see Chen et al., 2017).

A. Governance Decentralization

Governance decentralization is among the essential characteristics and values enacted by the cryptocurrency community (Bohme et al., 2015; Davidson et al., 2018; Mingxiao et al., 2017; Raskin 2013), which in fact advocates for more democratic digital ordering. Governance refers to the structure that supports transactions inside an organization, indicating the framework within which transactions are conducted (Williamson, 1979). Other researchers have interpreted cryptocurrencies governance as "constitutional" regimes, which encompass the rules and the rules about making rules (Alston, 2019; Berg, Berg, and Novak, 2020). Governance decentralization in cryptocurrency protocols reflects the degree to which the actions of and transactions between agents are possible and practical without the control or authorization of a reduced group of individuals (Benkler, 2010). While the current wave of cryptocurrency protocols tend to be overall more decentralized than other currencies (e.g. fiat, cryptographic, or virtual currencies) (Chaum, 1983; European Central Bank, 2012); inside the cryptocurrencies sphere, there are different degrees of decentralization. Three dimensions may affect cryptocurrencies' governance decentralization level, which are roles permissiveness, validation network size, and resource expenditure.

Inside cryptocurrency protocols, there are three prominent roles: users, developers, and validators. Users conduct transactions and store value within the network (Pereira et al., 2019). Developers have the technical ability to maintain the underlying code and to suggest code amends and upgrades, defining the future directions of the project (Berg et al., 2020; Pereira et al., 2019). Validators record and verify transactions, obeying to a specific consensus

mechanism. Some researchers see developers and validators as belonging to the same group (Alston, 2019). These two groups overlap as validators tend to have technical and functional knowledge about the protocols, voting, proposing, debating, accepting, or rejecting suggestions to upgrade the code, being often developers (Pereira et al., 2019; Berg et al., 2020). Therefore, these two groups of participants perform governance functions on behalf of users. Their decisions affect core definitions of the protocol, the validation process, the incentives of network participants, and the comparative ability of a given blockchain to achieve its network objectives (Alston, 2019). In this paper, we suggest that the level of decentralization of a protocol depends on the degree to which each role is permissionless.

High governance decentralization means that the tasks of decision-making and transaction performance, recording, and validation belong to many participants across the network. In these open, permissionless networks, anyone can join the network to make P2P transactions, which are validated by an independent pool of validators, who follow a consensus mechanism that allows reaching agreement on transactions (Davidson et al., 2018). Additionally, the community of developers can also suggest and vote on amendments to the code and new updates, or even fork the code, since these cryptocurrency protocols also tend to be open source. Cryptocurrency incentives fuel participation and coordination, securing the maintenance of the platform without the need for a third party to verify and record transactions and to maintain and take decisions about the future of the project (Davidson et al., 2018). Such a level of governance decentralization follows Nakamoto's Bitcoin ideal of creating a permissionless network, which everyone can join to perform transactions, validate them, or update and change the code (Böhme et al., 2015; Nakamoto, 2008).

Low governance decentralization means that there is a group of authorized nodes in the network responsible for decision-making, transaction performance, and/or recording and validation. Cryptocurrency protocols that encompass delegated Byzantine fault-tolerant

(DBFT) consensus mechanisms, and similar variants, tend to present a few central nodes that "control" the network (Crain et al., 2018). Such control can be exerted at transaction validation, data recording, and decision-making levels. One application example is NEO, a blockchain-based platform that aims to enhance the "smart economy" (NEO Whitepaper, 2019). In this project, a voting mechanism picks the validators (Neo Developer Guide, 2020; EOS Developer Guide, 2020), and only a group of authorized nodes in the network are responsible for recording and validating transactions. Additionally, the decision-making is also centralized in the NEO foundation (NEO, 2019).

In this paper, we build the argument that the degree of permissiveness across developers, users, and validators roles—whether the roles are open to everyone or restricted to a defined group—is one of the features that help to determine the level of governance decentralization of a protocol. Therefore, the higher the number of permissionless roles, the higher the level of decentralization in cryptocurrency protocols.

> *P1a. Cryptocurrency protocols that display permissionless roles across users, validators, and developers tend to have a higher governance decentralization than cryptocurrency protocols that present permissioned functions for users, validators, and/or developers.*

While the number of permissionless roles constitutes a good proxy of governance decentralization, it is meaningless if the validation network is relatively small and/or if a small number of nodes concentrates the validation and data storage processes (Wang et al., 2019). Validators, who record and verify transactions obeying a specific consensus mechanism, are essential as they replace a centralized actor in validating transactions and storing data (Pereira et al., 2019). There are three main reasons behind centralized validation networks. First, the validation roles are restricted to a select group of nodes. Second, the number of validation nodes is small in the consensus protocol despite being permissionless. Third, because despite

displaying permissionless and unrestricted numbers of validation nodes, there are accessibility issues due to high resource expenditure that can function as a barrier to entry (see proposition P1c). For whatever reason, if the group of validators is relatively small, such a network would be similar centralized governance modes.

The main risk of having a reduced validation network is the concentration of power around few validation nodes that can collude, alter the state of the network, or block certain transactions or addresses, resembling centralized governance systems (see Benkler, 2010). Such misbehaviours are less likely to occur in more extensive validation networks, as it is more difficult for a larger group of validators to agree and coordinate to misbehave. Therefore, cryptocurrency projects that present wider validation networks are more decentralized than those that display smaller validation networks. Two opposing examples are Stellar, a DBFT protocol, which has around 73 validation nodes (Stellarbeat.io, 2019), and Bitcoin, a PoW (Proof-of-Work) protocol, which validation network encompasses about 10.000 validation nodes (Bitcoin, 2019).

> *P1b. Cryptocurrency protocols that present more extensive validation networks tend to be more decentralized than cryptocurrency protocols that display smaller validation networks.*

Beyond the number of permissionless roles and the network size of validation nodes, the number of nodes is also determinant for the level of decentralization of any cryptocurrency protocol. If the groups of users, validators, or developers are relatively small, despite being permissionless and anyone being able to participate, control would be centralized in this small group, resembling centralized governance modes. An important factor that can contribute to raising barriers to entry in a network is resource expenditure, which relates to the resources spent to access, update, perform, record, or validates transactions. Resource expenditure encompasses requirements in terms of specialized hardware or complicated software to

perform, record, or validate transactions (Gipp et al., 2015), and also computational power (i.e. electricity used to validate transactions and data storage) (Gipp et al., 2015) or staking power (amount of tokens/coins) to validate transactions. Low resource expenditure reduces barriers to entry, allowing more members to join the network, and bigger networks tend to be more decentralized than smaller networks, *ceteris paribus*.

The cryptocurrency projects that encompass PoS (Proof-of-Stake) are an excellent example of cryptocurrency protocols that enhance decentralization through their potential to attract large networks due to their low resource expenditure. However, while PoS consensus mechanism does not require specialized hardware or complicated software to perform, record, or validate transactions, they do require staking power, demanding participants to stake some of their tokens to become validators. Nevertheless, even if the stakes needed to validate a transaction are very high, staking power is a resource intrinsic to the network, as staking require owning tokens/coins that store value on itself. For this reason, PoS based cryptocurrency protocols have the highest potential to score high in governance decentralization, despite not being the most adopted protocol at the date of writing and no application case has yet achieved a network size bigger than Bitcoin, for example. Nevertheless, we argue that PoS application protocols would tend to attract more extensive networks theoretically.

On the other extreme, there are PoW protocols, which require specific hardware, and computational power (high resource expenditure) which is a resource extrinsic to the protocol, being burned in the process of transaction validation. For example, Bitcoin, a PoW protocol, requires ASIC machines, which are expensive, and requires high-energy consumption for transaction validation, scoring high on resource expenditure. This example highlights that despite displaying permissionless roles and being designed to be decentralized, the reality is that validation roles are not easy to access in Bitcoin protocol and mining power concentrates in a few large mining pools (Romiti et al., 2019). Still, Bitcoin is among the existing protocols

the more decentralized one due to its age, relative high adoption, and big validation network, however, the increased resource expenditure may prevent this network of reaching fully decentralized governance.

P1c. Cryptocurrency protocols that display low resource expenditure tend to be more decentralized than cryptocurrency protocols that present high resource expenditure.

B. Security

The security aspect of cryptocurrency protocols is a significant area of research, as security is essential to any protocol that wants to guarantee the disintermediation of transactions. A secure protocol needs to be fault-tolerant, resilient, and immutable. While fault-tolerance is the ability to survive to several failures before a disconnection (Najjar and Gaudiot, 1990); resilience is the capability of the application to recover to an acceptable operational condition after it faces an event, such an attack (Infosys, 2019). Finally, immutability entails that the current or previous state of the distributed ledger cannot be modified once created.

There are two main general types of attacks against cryptocurrency protocols: spam and "51% attacks", which may have short or long-range[1]. Short-range attacks encompass Spam attacks, like DDoS (Distributed Denial of Service) and DNS (Domain name system) attacks, which happen when a targeted server is flooded with superfluous requests to purposefully overload the system and prevent the provision of regular service to other users, exploring the vulnerabilities of the server. Several exchanges of Bitcoin and Ethereum (PoW based cryptocurrency protocols) suffer from DDoS attacks and DNS attacks frequently, hampering the service available to users. For instance, with Bitcoin, such attacks can cause a devaluation of the cryptocurrency, loss of mining rewards, or even closure of cryptocurrency exchanges

[1] For our analysis, we ignore social attacks, such as phishing, malware, or direct wallet hacks. Social attack vectors will always exist, as long as there is a password and, therefore, an incentive to the attacker to steal that password. Social attacks are not protocol-specific, meaning that such attacks may happen independently of the technology or protocol.

(Saad et al., 2019). Another type of frequently discussed attacks and potentially the most harmful long-range attacks to cryptocurrency protocols are "51% attacks". Such attacks happen when validators can reverse transactions and initiate double-spending, which means that they would be able to spend the same coin multiple times. Such attacks can also entangle exclusion and modification of the order of the transactions; selectively withholding mined blocks and only gradually publishing them (selfish mining); provision of contradicting block and transaction information to different blockchain network nodes (eclipse attacks), hampering the normal mining operations of other miners (Li et al., 2017; Gervais et al., 2017). So far, cryptocurrencies such as Ethereum Classic, a hard fork of the Ethereum protocol, or Vertcoin, an alternative implementation of the Bitcoin protocol focusing on increased privacy, both have been successfully 51% attacked, more than once (Coindesk, 2020).

For a cryptocurrency protocol to be secure, it should guarantee both network fault-tolerance and resilience to be short and long-range attacks, preserving the immutability of the distributed ledger in the long-range (see Kewell et al., 2017; Najjar and Gaudiot, 1990). There are technology and organizational features that can affect cryptocurrency protocols security, which is resources expenditure (computational power and staking power), TPS (number of transactions per second), and validation network size.

Resource expenditure in transaction validation in one of the factors that may affect protocols' fault-tolerance and resilience to "51% attacks" that can compromise the immutability of the protocol in the long run. Resource expenditure may encompass the resources needed to validate and store transactions in a network, entangling both computational powers (energy/electricity spend to validate and store transactions) or staking power (amount of tokens/coins needed to be at stake to validate transactions). As validators may need to spend resources to validate transactions, if they intend to attack the network, they would need to control more than (at least) 51% of the validation resources of the network. Therefore, higher

the resource expenditure to validate transactions, more difficult is to actors to control 51% of the network, and higher tend to be the fault-tolerance and resilience of the protocol and, therefore, higher the security.

PoW based cryptocurrency protocols, for example, are based on cryptographic calculations that make miners spend energy to solve computational problems to find a hash that links all blocks in the blockchain. To perform a "51% attack" in PoW protocols, validation nodes need to control 51% of the hashing power. This means that, if the attacker wants to keep mining on the orphan chain, they need to continuously spend energy to maintain control to be selected over and over again to create a block to be accepted as valid on the main chain. Such energy expenditure is continuous, which can easily reach prohibitive levels. Therefore, since attackers cannot sustain the attack indefinitely due to resource investment, PoW based protocols tend to display a higher resilience and fault-tolerance when compared with other similar networks that endorse different protocols (e.g. DBFT or PoS). An example of PoW application protocol is Bitcoin, which resource expenditure in terms of computational power (energy/electricity) is one of the highest of the cryptocurrency sphere, being simultaneously one of the most secure and resilient to "51% attacks", as such would achieve prohibitive values. One of the most significant criticisms to Bitcoin concerns the amount of energy spent to maintain and run the protocol (O'Dwyer and Malone, 2014).

Another way to validate transactions in cryptocurrency protocols is by using staking power, as is the case of PoS protocols. Even though no double-spend attack has ever been successful in this type of protocol up to this date, we argue that the long-term impact of a hypothetical successful attack could be devastating. In the PoS case, there is no high-energy expenditure; however, there is a need for staking power. The vulnerability of PoS protocols relates to how much stake is needed to validate transactions and the amount of investment required to acquire such tokens/coins to control the network. Still, suppose an attacker holds more than 51%

tokens/coins in a PoS protocol. In that case, there is no way to exclude the attacker from the network, and staking power will forever be tilted in one direction unless the protocol excludes the attacker's coins from the network (hard fork). Additionally, this expenditure to maintain the attack through acquiring 51% of staking power is only incurred once, not continuously like in PoW protocols. Theoretically, if a PoS protocol is attacked successfully, a hard-fork would be required to fix it, at the expense of the immutability of the ledger; while in PoW, the attacker eventually would run out of resources.

DBFT protocols are among the most adopted protocols. These federated protocols are more straightforward to attack due to the low resources expenditure to store and validate transactions. In DBFT protocols, validation is reached through an agreement among several central authority nodes. In this case, the resource expenditure is considerably low and staking power is not required as well; therefore, attacks are more likely to happen. Hypothetically, suppose a DBFT validation network has few validation nodes. In that case, the possibility that few nodes collude and control 51% of the network is real, and the colluding nodes could potentially create additional currency, access to private data, hack private keys, and censor transactions given they control the majority of the network. We, then, argue that protocols that require higher resource expenditure tend to be more fault-tolerant and resilient to 51% attached, being, therefore, more secure than protocols that have low resource expenditure requirements.

> *P2a. Cryptocurrency protocols that require higher resource expenditure to validate transactions tend to display higher security, then cryptocurrency protocols that require lower resource expenditure.*

Cryptocurrencies' TPS (number of transactions per second that a protocol can perform on average) can also play a significant role in dictating how resilient and fault-tolerant a protocol is against spam and 51% attacks. Such attacks are possible because decentralized network nodes tend to be asynchronous, meaning that information might take some time to arrive from

one node to another (Crain et al., 2018). This time-lapse, also called propagation delay, can lead to the situation that during the validating process, two or more coinciding blocks can be created at the same time, originating a parallel chain of blocks (aka orphaned blocks). As long as more than one chain is valid, different nodes may accept different versions of the blockchain, and it becomes harder for a new node to know the "truth" of the ledger. The existence of orphaned blocks may increase the likelihood that transactions are lost or/and double-spend and "51% attacks" may happen. Eventually, the orphaned blockchain will be void and transactions cancelled. Nevertheless, such events affect the immutability of the ledger and users' confidence, destroying the value of timestamped transactions, the faith of the users, and the security of the network.

TPS can be enhanced by increasing the block weight or decreasing the block-time. Block weight encompasses the size of the block in terms of bytes and bits. Each transaction performed under a cryptocurrency protocol has a specific size in bytes and bits. As a reference point, Bitcoin transactions size may vary between 225 bytes and a maximum of 4 MB (Nakamoto, 2008). Block-time corresponds to how much time it takes a block to be added to the chain of blocks (blockchain). For example, the Bitcoin protocol requires, on average, 10 minutes for a partnership to be created and added to the blockchain (Nakamoto, 2008). On the one hand, the bigger the block weight, the longer the block confirmation period, and higher the time-lapse (or propagation delay), which increases the likelihood of orphaned blocks and "51% attacks". On the other hand, the shorter the block-time, more often, the information is sent to the nodes, being the nodes' synchronization requirements higher, leading again to propagation delays and synchronizing issues.

A much-discussed potential solution for Bitcoin's (PoW protocol) low TPS (7 transactions per second) is to increase the size of its blocks. Unfortunately, as explained, this solution leads to higher propagation delays, which again increases the probability of orphaned blocks and the

risk of attacks (Kokoris-Kogias et al., 2016). Contrasting examples are NEO (a DBFT application) and EOS (delegated PoS protocol), which display higher TPS. For reference, NEO can produce up to 10,000 TPS, whereas EOS close to 4,000 (NEO Developer Guide, 2020; EOS Developer Guide, 2020). Both protocols theoretically possess a higher risk of creating orphan blocks and of suffering from "51% attacks". As exposed, increasing TPS may entail propagation delays and synchronization issues, which may lead to orphan blocks and consequently increase the likelihood of 51% attacks, reducing the security of the protocol.

P2b. Cryptocurrency protocols that display lower TPS (transactions per second) tend to be more secure than cryptocurrency protocols that present higher TPS.

The size of the validation network influences not only governance decentralization but also the protocol's security and the probability of a successful attack on the network. One of the main concerns of the cryptocurrency community regarding security is that a node or a group of colluded nodes control over 51% of the validation power of the network, as such an entity could effectively control the system by sustaining the longest chain and conduct "51% attacks" (Li et al., 2017; Gervais et al., 2017). In this paper, we argue that in cryptocurrency protocols that display more extensive validation networks (Croman et al., 2016), the validation power will be more distributed, decreasing the likelihood that a single node or collusion of nodes attack the network, thus improving the overall security of the protocol. An example worth mentioning is EOS, the delegated PoS based blockchain protocol that suffered a validator collusion attack (Cointelegraph, 2018). The claimants accused the EOS block producers, the entities responsible for minting blocks, of colluding with one another by mutual voting. Such type of colluding behaviour that endangers the security of the network is more likely to happen in smaller than bigger validation networks.

P2c. Cryptocurrency protocols that display more extensive validation networks tend to be more secure than cryptocurrency protocols that communicate smaller validation networks.

C. Scalability

Scalability represents the capability of a network to handle a growing amount of work or its potential to be enlarged to accommodate that growth (Ethereum, 2019). Scalability entangles three main dimensions: transaction volume, speed, and scope. Transaction volume refers to a network capacity to increase the number of outputs, maintaining the same number of inputs. Transaction processing speed is the capacity for a particular network of nodes to process more inputs during the same period. Speed augments as the faster processing time for the same set of transactions given the same network inputs per transaction. Finally, transaction scope is the network capacity to process the same number of information with additional data parameters to increase the overall network functionality (Investopedia, 2020; Grayblock, 2018). A system is considered scalable if it is capable of increasing its total output under an increased load when resources (typically hardware) are added; if it can process more inputs per second; or if it can produce additional functionality as an output, per the same number of inputs. TPS and validation network size are features that have implications for scalability.

Cryptocurrency protocols' TPS has a direct impact on the scalability potential of the network. Protocols that display higher TPS can conduct more transactions per second, what is relevant when such protocols ambition to be worldwide adopted. To increase TPS, one might raise the block weight of decrease the block-time. Larger blocks are likely to contain a higher number of transactions, and shorter block-time is expected to accelerate the number of blocks produced, increasing the numbers of transactions validated per second. Cryptocurrency protocols may display different block weight and time, and even some variations in terms of fees, and the absence of strict block weight or time, therefore, the best comparison measure is

indeed TPS. Regarding existing protocols, one extreme encompasses PoW protocols, such as Bitcoin, which currently can perform seven transactions-per-second on average (Nakamoto, 2008), and Ethereum, which display around nine transactions-per-second; on the other extreme, DBFT protocols, such as Stellar and Neo can do a maximum of ~10,000 transactions-per-second (Mazieres, 2016; NEO Whitepaper, 2019), having the higher potential for scalability.

P3a. Cryptocurrency protocols that display higher TPS tend to be more scalable than cryptocurrency protocols that have lower TPS.

Cryptocurrency protocols' distributed ledgers require that every validation node keeps a complete or partial copy of the ledger data locally, forming a distributed ledger. However, as the number of users increase and consequently, the number of transactions, the amount of data transmitted via network bandwidth and stored on node devices increases. Keeping and maintaining such large amounts of data synchronized at every node of an extensive validation network is a bottleneck for the network growth. Additionally, messages and transactions are delivered in a flood fashion, which means that devices must be woken up frequently to process received events, thereby increasing battery consumption dramatically (Wei-hong et al., 2017). The limitations in terms of network bandwidth, data storage, and energy consumption, which may increase propagation delays, inevitably offer challenges to protocols' scalability.

One possible way to address propagation delay issues to increase scalability is by decreasing the number of nodes participating in the validation network. The smaller the number of nodes, the faster is the synchronization among them, and higher is the network ability to scale. The reduction of the validation network to increase scalability is often achieved through delegation of validation power to a small group of validators or through the creation of permissioned nodes that validate and store transactions. For example, Stellar a DBFT protocol can process between 1000 and 10,000 TPS, being a reasonably scalable protocol. However, the validation network has only 70 validation nodes that are vetted institutions only (Stellarbeat.io, 2019).

P3b. Cryptocurrency protocols that display smaller validation networks tend to be more scalable than cryptocurrency protocols that have larger validation networks.

IV. CRYPTOCURRENCY PROTOCOL CONSTELLATIONS

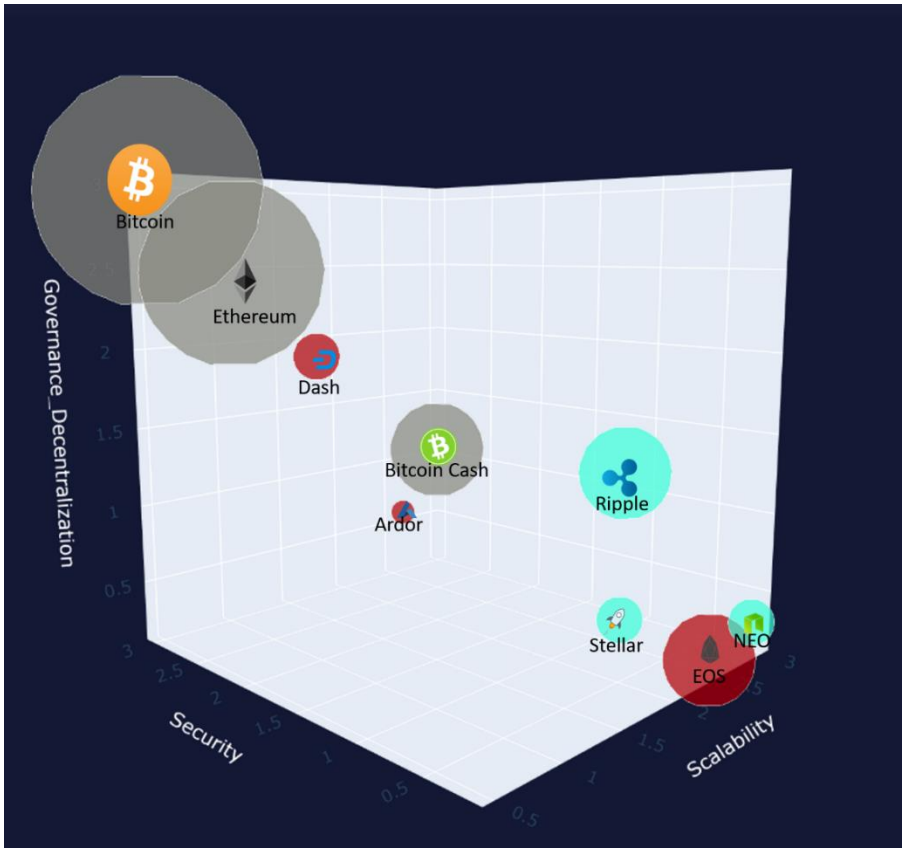
The different cryptocurrency protocols share a number of characteristics, such as cryptography, cryptocurrency incentives, distributed ledgers, and consensus mechanisms that distinguish them from other protocols and from other digital currencies; however, inside the universe of cryptocurrency protocols, there are significant differences across governance decentralization, security, and scalability. As exposed throughout our propositions, organizational and technological features as roles permissiveness, validation network size, resource expenditure, and TPS can have opposing effects on governance decentralization, security, and scalability, creating trade-offs among these three fundamental dimensions. For example, while larger validation networks positively influence governance decentralization and security, it has a negative influence on scalability. Similarly, a high resource expenditure increases security but decreases governance decentralization, and a high TPS increases scalability but decreases security. These inherent trade-offs make difficult or nearly impossible, considering the current state of the technology, for a protocol to be decentralized, secure, and scalable at the same time. Whether a cryptocurrency will achieve more decentralization, security or scalability is partially defined by its consensus mechanism, which dictates the rules that validators and users must follow to participate in the network, building agreement among a network of mutually trustless participants. Consensus mechanisms are, therefore, the most defining element of cryptocurrency protocols.

At this date, three main consensus protocols have been implemented in cryptocurrency projects: PoW, PoS, and DBFT (Shijie and Lee, 2019)[2]. However, it is important to note that,

[2] We used the term "main consensus mechanism" to describe the most widely adopted protocol implementations. Looking at the top-10 cryptocurrencies, around 50% are PoW, while 30% are PoS, and the remaining 20% are DBFT (Coinmarketcap, 2020-March, 2020).

while some cryptocurrency projects instantiate pure versions of these consensus mechanisms, others integrate variations across roles permissiveness, validation network size, resource expenditure, and TPS. As an analogy, we discuss three constellations of cryptocurrency projects (PoW, PoS, and DBFT), in which each constellation represent a group of projects that share the same consensus mechanism, as constellations of stars share the nearby space. Then, we mapped the constellations of cryptocurrency projects in the three-dimensional space of governance decentralization, security, and scalability (see Figure 1 and Table 2), applying the propositions proposed previously and discussing how each protocol and project manage the trade-offs.

FIGURE I
CRYPTOCURRENCY PROTOCOLS CONSTELLATIONS



Bubble sizes represent adjusted market capitalization (data from November 2019). PoW constellation: Bitcoin, Ethereum, BitcoinCash; PoS constellation: Dash, Ardor, EOS; DBFT constellation: Ripple, NEO, Stellar

TABLE 2
CRYPTOCURRENCY PROTOCOLS DATA

	Market cap ($, billions)*	Consensus mechanism	Network size in validation nodes	TPS
Bitcoin	170.0	PoW	9354	7
Ethereum	20.0	PoW	6711	9.3
Bitcoin Cash	5.0	PoW	1453	110
Ardor	0.1	PoS	131	110
Dash	0.6	PoS	4430	34
EOS	3.0	PoS	21	3996
Ripple	13.0	DBFT	1011	1500
Stellar	1.2	DBFT	73	1000-10000
Neo	0.7	DBFT	7	1000-10000

*Values of November (CoinMarketCap, 2019-block explorers)

A. PoW Constellations

PoW is a consensus mechanism based on cryptographic calculations that make miners spend energy to solve computational problems, in order to find a hash that links all blocks in the blockchain (Fani et al., 2019). PoW protocols require resource expenditure, specifically computational power, as energy needs to be spent to validate transactions. In a case of a 51% attack on the network, the attacker needs to spend a prohibitive amount of energy to keep the orphaned block, which can reach prohibitive levels (Nakamoto, 2008; Biswas and Muthukkumarasamy, 2017) (see P2a). Therefore, among the three main consensus mechanisms, PoW is the one that favours security the most. In the following paragraphs, we will describe cryptocurrency protocols that include PoW, which are Bitcoin, Ethereum, and BitcoinCash (see Figure 1).

Bitcoin: Bitcoin was designed to be used as digital cash and gold, and it is the oldest and first implementation of a fully working PoW system, based on the SHA256 encryption algorithm (Nakamoto, 2008).

Bitcoin presents permissionless roles across users, validators, and developers (P1a), and a large validation network with 9350 validation nodes (P1b) (Blockchair, 2019), scoring high in governance decentralization. However, Bitcoin also scores high in resource expenditure (P1c),

which prevents it from realizing its full decentralization potential. Since 2013, Bitcoin miners (validators) began to use computers designed specifically for mining cryptocurrency as efficiently as possible (called ASICs), which are expensive and need to be upgraded often. In addition, validators also need to spend a high amount of energy to solve computational problems to find a hash that links all blocks in the blockchain (Fani et al., 2019) to validate blocks of transactions. Despite Bitcoin was initially designed to be "the decentralized" network, the high resource expenditure (see P1c) has created an inverse incentive, resulting on some level of concentration of validation power in big mining pools (Romiti et al., 2019). Nevertheless, age, wide adoption, permissionless roles and validation network size reinforces Bitcoin's governance decentralization, making it one of the most decentralized protocols in existence.

Bitcoin also scores high in security due to high resources expenditure (P2a), low TPS of around 7 (Nakamoto, 2008) (P2b), and relatively large validation network (see P2c). As explained previously, cryptocurrency protocols with lower TPS (smaller block size and longer block time) tend to be more secure, as the long block time allows nodes to synchronize the information on transactions and ledger state each time a block is produced, minimizing propagation delay issues. Additionally, Bitcoin currently possesses a high hash rate. The higher the hash rate, the higher is the resource expenditure, the more difficult it is to perform and maintain a 51% attack. All these factors explain why Bitcoin is one of the most secure of the cryptocurrency protocols. Alternatively, Bitcoin is one of the least scalable protocols displaying small TPS (block weight of around 1.2 MB, and block time around 10 minutes) (Nakamoto, 2008) (P3a). In the Bitcoin case, security and decentralization are achieved at the expense of scalability (Fani et al., 2019).

Ethereum: Ethereum was one of the first ICOs (initial coin offerings) in the cryptocurrency space that took place during 2015. The goal of this cryptocurrency is to become the first

decentralized world computer, meaning that any user can deploy dApps or decentralized applications over the Ethereum protocol by paying a fee in its native blockchain cryptocurrency, Ether (Ethereum, 2019; Liquid, 2018).

Much like its peer Bitcoin, Ethereum also scores relatively high in decentralization as it possesses permissionless roles (P1a) and a large validation network of 6500 nodes (Blockchair, 2019) (P1b), making it the second most decentralized network. While Ethereum does not require particular hardware to operate, being "GPU-friendly," validators still need to spend energy to validate transactions (Ethereum, 2019) (see P1c). This has been an issue to improve the decentralization of the project and one of the main reasons motivating the transition of Ethereum from PoW to PoS since in PoS, the validation process is through staking tokens[3]. Currently, Ethereum presents a relatively low TPS (between 9 and 50) (Etherscan, 2019; Ethereum, 2019) (P2b); however, it presents a lower resource expenditure than Bitcoin, as its hashing power is lower, which makes it easier to attack the network and compromise its security (P2a). It is estimated that the cost of attacking Ethereum through 51% attacks would be around half the cost of attacking Bitcoin (Exaking, 2019), making it less secure than Bitcoin, but still one of the most secure cryptocurrencies in the space. Much like Bitcoin, in Ethereum, security and decentralization are achieved at the expense of scalability.

Bitcoin Cash: Bitcoin Cash (BCH) is an alternative cryptocurrency, or altcoin, created in mid-2017 from a hard fork of Bitcoin. Increased fees on the Bitcoin network in December 2017 induced some in the Bitcoin community to enable BCH, which runs on SHA256; however, it presents an increased block weight (Bitcoin Cash, 2019).

Much like with other PoW protocols, the governance roles of BCH are permissionless (P1a), and its validation network encompasses 1400 validating nodes (Blockchair, 2019) (P1b). BCH

[3] At the moment of writing, Ethereum community is planning to transition from PoW to PoS consensus. Still, it will keep running a PoW protocol for the foreseeable future (Ethereum, 2020).

also display high resource expenditures, as it requires ASIC hardware (P1c). Hence, Bitcoin Cash is less decentralized than previous PoW protocols, mainly due to smaller validation networks, lagging behind both Ethereum and Bitcoin. Bitcoin Cash can perform 110 TPS (Bitcoin Cash, 2019), a bit higher than the other PoW protocols. This increase in block size potentially leads to network latency problems, making Bitcoin Cashless secure than the other PoW protocols presented in this paper (P2b). Another factor that has contributed to Bitcoin Cash's lower security is its hash rate, which is 3% of Bitcoin's (P2a). Finally, in terms of scalability, of the cryptocurrencies, we studied Bitcoin Cash is the PoW that shows the best results. It outperforms both Bitcoin and Ethereum in terms of TPS (P3a). To achieve this result, Bitcoin Cash loses a degree of both decentralization and security.

B. PoS Constellations

PoS consensus algorithm was invented by the South African Sunny King, during the late 1990s, before PoW was created by Nakamoto. Unlike PoW, which involves resource expenditure to solve a cryptographic puzzle, PoS requires participants to stake some of their tokens in order to become network validators (Fani et al., 2019). To prevent misbehaviour, PoS systems penalize any agent who tries to attack the network, by removing the agent's stake. As anyone with a stake can participate in the network (P1a) and validation does not require high resource expenditure (because it does not involve spending energy in the mining) (P1c), PoS is theoretically the protocol with the highest decentralization potential. However, owing to existing network sizes, which are sometimes reduced, and PoS variations (e.g., votes delegation), its decentralization potential has not yet been fully realized. In this paper, we will discuss Dash, EOS, and Ardor PoS applications.

Dash: Dash is a cryptocurrency that aims to be an untraceable, fast digital currency, using mainly a PoS protocol. Dash is currently mostly used in countries like Venezuela, where people

need to conduct transactions quickly with privacy and confidentiality due to strict government regulations (Dash, 2019; Baker, 2019).

Theoretically, Dash displays permissionless roles across users and validators. However, while there is no need for acquiring special equipment or spending computer power, anyone who wants to enter the master nodes/validation network needs to pay a stake in Dash, which can be out of reach for most of the people (staking power) (P1c). Furthermore, governance decisions are not open to everyone but instead just to the masternode network through their voting rights (P1a). Currently, there are more than 4430 nodes (Blockchair, 2019) validating transactions on the Dash network, which is a relatively large validation network (P1b); however, the entry and voting requirements make it less decentralized than Bitcoin or Ethereum, for example.

Dash displays medium resource expenditure (P2a), and 34 TPS (Dash, 2019) (P2b), which contributes towards increased security. However, Dash's technology itself is not private but instead a mix of tumblers and cryptocurrency features. This means that, if a masternode is attacked, user information (addresses and transaction details) could be leaked. Additionally, the fact that masternodes "stake" to enter the network means that a relevant percentage of masternodes can, in fact, be controlled by a group of colluding agents (P2c). In this sense, Dash is less secure than Bitcoin or Ethereum, for example. Finally, Dash block size is currently 2 MB, and it has a TPS of 34 (Dash, 2019), making it more scalable than traditional PoW cryptocurrencies, but less secure.

EOS: EOS.IO uses a blockchain architecture designed to enable vertical and horizontal scaling of decentralized applications, by creating an operating system-like construct upon which applications can be built. EOS uses Delegated Proof-of-Stake in which anyone who holds tokens on the platform may select one of 21 block producers through a continuous approval voting system (EOS.IO, 2019).

EOS uses a system of delegation of validation power to a few nodes inside the network contributes toward centralization, in this case concentrating validation in 21 nodes (Blocks.io, 2019) (P1b). Such conditions make EOS one of the most centralized PoS networks, after Tron and BitcoinSV. Both the reduced number of nodes inside the validation network (P2c) and high TPS (4000 TPS) (P2b) contribute towards low security among PoW protocols. However, what EOS loses in decentralization and security, it gains in scalability, as it is able to conduct millions of transactions per second (4000 TPS) (P3a), through a reduced validation network (EOS.IO, 2019) (P3b).

Ardor: Ardor was created to allow businesses to use a public blockchain, developing and delivering blockchain technology that developers and business can implement in an easy and scalable manner. Ardor is a pure PoS algorithm, the first to ever be created, where any user can validate transactions by committing some number of NXT tokens (stake) in order to forge (validate) blocks (Jelurida, 2019).

While usage and validation in Ardor are open to everyone, development is restricted to the Ardor team (P1a). Ardor scores low in resource expenditure (P1c), however, its validation network counts with 131 nodes, being relatively small (P1b) (ArdorPortal, 2019), presenting a medium governance decentralization, despite its potential to be highly decentralized in the future. In terms of security, Ardor can process around 110 TPS (Jelurida, 2019), which lags far behind EOS. However, Ardor is more secure than the previous cryptocurrency PoS protocols, simply because it is harder to coerce a far greater number of speakers to collude without voting rights. In addition, any attack on the network would only work if a staker possessed at least 51% of the token supply, which is practically infeasible given that price fluctuates with demand (P2c). Nevertheless, Ardor, despite being less scalable, is still much more secure and decentralized than EOS, for example.

C. DBFT Constellations

DBFT is a federated consensus, meaning that the network reaches consensus through agreement/voting among a number of central authority nodes. While proof-based consensus requires some sort of proof, may that be work (PoW) or stake (PoS), among others, federated consensus models rely on both reputation and authority of the nodes? Essentially, the latter pushes for some centralization in the coordination mechanism, as there are hierarchies between those who are allowed to vote on and validate new blocks and those who are using the chain for transaction purposes only. These federated consensus networks are not public to everyone, meaning that only a few permissioned nodes can participate in the consensus through voting (Christophi, 2019). DBFT consensus mechanisms and related variations are among the most scalable protocols of the cryptocurrency space (see Crain et al., 2018; Crain et al., 2017), as they tend to display high TPS (P3a) and small validation networks (P3b). In the following sections, we describe Ripple, Stellar, and NEO (see Figure 1).

Ripple: Ripple, originally released in 2012, is a real-time gross settlement system (RTGS), currency exchange, and remittance network. It uses a common public shared ledger, which is managed and maintained by a network of independent validating nodes that can belong to anyone from individuals to banks. Unlike the other cryptocurrency protocols set out in this paper, Ripple does not use blockchain as a data infrastructure; it uses HashTree to summarize data into a single hash that is compared across nodes to provide consensus (Schwartz et al., 2018; Liquid, 2018)

In terms of governance decentralization, Ripple accepts new validators to join the network; however, each validator must first be vetted by the community; therefore, this role is somewhat permissioned (P1a). Ripple display low resource expenditure (P1c) what may have contributed to fairly decentralized validation network (over 1011 nodes) (XRPcharts, 2019) (P1b), making it a fairly decentralized BFT network despite the permissioned access to validation roles.

Regarding security, Ripple heavily relies on a unique node list (UNL) to censor malicious validators, as any validator not in another validator's UNL is ignored. Validators vote on pending transactions, and only transactions accepted by at least 80% of validators are placed in the next block (Schwartz et al., 2018). Ripple, thus, display a low resource expenditure (P2a), a high TPS (1500 TPS) (P3a) (Schwartz et al., 2018), but a fairly large validation network (P2c) which make it more secure than other DBFT protocol application. On the other hand, Ripple is one of the most scalable projects in the cryptocurrency sphere due to its high TPS (P3a).

Stellar: Stellar, originally released in 2014, is a real-time platform that connects banks, payment systems, and people, allowing cross-boundary transactions between any pair of currencies, either digital or fiat, at very low costs, quickly, and reliably (Mazieres, 2016). Stellar's SCP is essentially an improved version of a Federated Byzantine Agreement, where Stellar Lumens (XLM) holders can become validators or vote for validators, making it a form of delegated BFT (dBFT). Despite introducing right voting systems, Stellar is quite centralized in terms of validating nodes, since—like Ripple—only vetted institutions can be a part of the consensus (P1a). At the time of writing, Stellar has only about 70 validating nodes (Stellarbeat.io, 2019), scoring low on governance decentralization (P1b). As governance is fairly centralized (P2c) and TPS very high (between 1000 and 10,000 TPS) (P2b), security is inherently lower than under other protocols. On the other hand, Stellar is able to perform between 1000 and 10,000 TPS (Mazieres, 2016), with a confirmation time between two and five seconds, making it a scalable protocol (P3a), a key selling point for DBFT protocols.

NEO: NEO is a decentralized application platform founded in 2014, with a vision to enhance the "smart economy" through blockchain and smart contracts to issue and manage digital assets. NEO develops user-friendly tools with known programming languages that allow developers to conceive and scale smart contracts in the NEO blockchain (NEO Whitepaper, 2019).

Despite NEO's low resource expenditure (as there are no transaction fees involved) (P1c), this cryptocurrency is one of the least decentralized of the studied cases, as NEO validators network is composed of a small number of centrally approved nodes (around 7) (P1b), and development is centralized in the NEO foundation (NEO, 2019) (P1a). Due to its very high TPS—1000 to 10,000—(NEO Whitepaper, 2019) (P2b) and small validation network (P2c), NEO display security issues. NEO losses in decentralization and security are compensated for by its scalability potential, as it is one of the most scalable projects presented in this paper.

V. DISCUSSION

In this paper, we explore governance decentralization, security, and scalability of cryptocurrency protocols. Our analysis of cryptocurrency protocols builds on and expands the CAP theorem (Brewer, 2000) that states that a decentralized storage system cannot have consistency, availability, and partition tolerance, all at once. Brewer's CAP theorem applies to distributed systems at large, and while some dimensions still apply to cryptocurrencies, others do not, as cryptocurrencies entangle different technologies on the top of distributed systems, as for example cryptography and consensus protocols, among others, which bring to the table different dimensions and implications for the trade-off.

We also expand Ethereum's scalability trilemma, which states that a blockchain cannot possess all three qualities: security, decentralization, and scalability simultaneously. While the scalability trilemma was developed in light of blockchain, specifically Bitcoin, and Ethereum, we have theorized and included other protocols, exploring the organizational and technology features that affect these dimensions and respective trade-offs. The organizational and technological variables that we theorize in this paper, not only allow mapping the general consensus protocols (PoW, PoS, and DBFT) alongside the three-dimensional space (governance decentralization, security, and scalability), but also the different protocol applications and variations.

Observing the picture of the constellations of projects implemented nowadays (see Figure 1), it is possible to observe that the Bitcoin and Ethereum, two PoW protocols, score the highest in terms of security (as predicted) but also in governance decentralization. In this specific case, PoW protocols Bitcoin and Ethereum are secure as they display high resource expenditure (mainly computational power) (see P2a), lower TPS (see P2b), and large validation networks (P2c), which reduce the likelihood of successful perpetrated attacks. Nevertheless, they also score high in decentralization, due to their permissionless roles (see P1a) and large validation networks (see P1b). For instance, Bitcoin and Ethereum present wide networks of users, developers, and validators, with over 9,000 and 6,000 validating nodes, respectively (values of quarter 1 of 2020) (Bitcoin, 2019). Such factors explain why these Bitcoin and Ethereum protocols are able to reach security and decentralization simultaneously. On the other hand, Bitcoin Cash, which is too a PoW protocol, ranks lower insecurity, than some PoS-based protocols, such as Dash. The reason is the fact Bitcoin Cash has a smaller validation network, which may increase the likelihood of being attacked (see P2c).

While it is possible for cryptocurrency projects to achieve security and governance decentralization simultaneously, it is more difficult to achieve scalability and security and/or governance decentralization simultaneously, considering existing technology. EOS (PoS based protocol) and Neo (DBFT based protocol) are such examples. While EOS displays a relatively high TPS (3996) (EOS.IO, 2019), it lacks decentralization and security. For instance, during 2019 there was a known issue with EOS validators colluding to remain validators, by agreeing on who was going to be voted as a validator in the next voting rounds. While EOS is indeed secure in terms of transactions being propagated, it is vulnerable to nodes collusion and attacks due to the centralization of validation power, ranking low in security (see P2c). Another example is Neo (a delegated BFT protocol), which is able to perform between 1000 to 10000 TPS and display a validation network of 7 nodes. Such examples show how scalability tends

to be achieved through small validation networks, which through enhance the chances that collusion behaviours and attacks occur, endangering the security of the protocol.

Limitations and further research

In this paper, we focused on organizational and technological features that influence governance decentralization, security, and scalability. However, other protocol features may also impact governance decentralization, security, and scalability. For example, TPS, in terms of block weight and time, has an impact on incentive systems of cryptocurrency protocols. As validators receive fees for validating transactions and in some cases, a reward for successfully adding a block to the chain, the level of reward and the block-time and weight will have an impact on their decision to be part of the network or not. Such aspect will influence the size of the network, and, therefore, decentralization. Other variables to consider could be tokens appreciation, as a higher token price means increased revenue for validators, which may attract more validators, increasing the validation network. Such dimensions may require further investigation as they entail a kind of egg-chicken problem, the size of the network increases because of the token appreciation, or the tokens' appreciation increase because of the increase of the validation network.

There are also other dimensions that we did not explore in this paper for the sake of brevity. Among these dimensions, we can name fungibility, accountability, privacy, confidentiality, and even anonymity. Within the cryptocurrencies sphere, there are concerns over whether the identity of users who make transactions is revealed. Bitcoin is an example of a "pseudonymous" currency, where encrypted accounts can theoretically be traced back to their owners while remaining anonymous for standard practical purposes (Nakamoto, 2008). Value can thus be held and exchanged in cryptocurrencies without the public disclosure of personal identity (Dierksmeier and Seele, 2018). What are the implications of different types of privacy and confidentiality? How do such variants affect the protocol, transactions, and users'

behaviours? Under which conditions should a protocol adopt flexibility in privacy and confidentiality? What are the costs and benefits of not being able to trace the flow of the money or limiting the amount of circulating coinage?

Nowadays, more than 4000 cryptocurrencies exist in exchanges (CoinMarketCap, 2019), representing a $300 billion market capitalization (Schroeder, 2019). However, we acknowledge that the scalability limitation denotes the current state of the technology, which is still in its infancy. Nevertheless, researchers shall not be demotivated by the current state of development but instead excited to start exploring, theorize, and test the similarities and differences that characterize the universe of cryptocurrencies.

REFERENCES

Alston, E., "Constitutions and Blockchains: Competitive Governance of Fundamental Rule Sets," *Centre for Growth and Opportunity at Utah State University*, Working Paper Series, 2019.

ArdorPortal, 2019. [Online]. Available at: https://ardorportal.org/monitor

Atzori, M., *Blockchain Technology and Decentralized Governance: Is the State Still Necessary?* 2015. [Online]. Available: https://ssrn.com/abstract=2709713

Baker, P, *Stress Test Shows Dash Scalable To 3M Daily Transactions,* Crypto Briefing, 2018. [Online]. Available at: https://cryptobriefing.com/scalable-dash-3m-transactions/

Barkatullah, J., and T. Hanke, "Goldstrike 1: Cointerra's first-generation cryptocurrency mining processor for bitcoin," *IEEE Micro*, vol. 35, no. 2, pp. 68–76, 2015.

Benkler, Y., "Capital, power, and the next step in decentralization," *Information Technologies & International Development*, vol. 6, SE, pp. 75,-77 2010.

Berg, A., C. Berg, and M. Novak. "Blockchains and constitutional catallaxy," *Constitutional Political Economy*, 1-17, 2020.

Biswas, K., V. Muthukkumarasamy, and W. L. Tan. "Blockchain based wine supply chain traceability system," *Future Technologies Conference*, 2017.

Bitcoin, 2019. Bitcoin Cash: Bitinfo charts, transactions. [Online]. Available at: https://bitinfocharts.com/comparison/bitcoin%20cash-transactions.html.

BitcoinCash, 2019. [Online] Available at: https://www.bitcoincash.org/.

Blockchain.com. 2020. [Online]. Available at: https://www.blockchain.com/en/pools

Blockchair, 2019. [Online]. Available at: https://blockchair.com/bitcoin-cash/nodes

Blocks.io, 2019. [Online]. Available at: https://bloks.io/#transactions

Böhme, R., N. Christin, B. Edelman, and T. Moore, "Bitcoin: Economics, technology, and governance," *Journal of Economic Perspectives*, vol. 29, no. 2, pp. 213–238, Spring 2015.

Brewer, Eric A. "Towards robust distributed systems". (Invited Talk) Principles of Distributed Computing, Portland, Oregon, July 2000.

Catalini, C., and J. S. Gans, "Some simple economics of the blockchain." Rotman School of Management Working Paper No. 2874598, 2017. [Online]. Available: https://ssrn.com/abstract=2874598

Chaum, D., "Blind signatures for untraceable payments," In Advances in cryptology, pp. 199-203. Springer, Boston, MA, 1983.

Chen, Y., H. Li, K. Li, and J. Zhang, "An improved P2P file system scheme based on IPFS and Blockchain," In *2017 IEEE International Conference on Big Data (Big Data)* (pp. 2652-2657). IEEE, 2017.

Chohan, U., "The limits to blockchain? Scaling vs. decentralization." Discussion Paper Series: Notes on the 21st Century (CBRI), 2019. [Online]. Available: https://ssrn.com/abstract=3338560 or http://dx.doi.org/10.2139/ssrn.3338560

Christofi, G. "Study of consensus protocols and improvement of the Delegated Byzantine Fault Tolerance (DBFT) algorithm." Universitat Politècnica de Catalunya, 2019.

Coindesk, "51% Attacks," 2020. [Online]. Available at: https://www.coindesk.com/tag/51-attack

Coinmarketcap, "Top 100 Cryptocurrencies by market Capitalization," 2020. [Online]. Available at: https://coinmarketcap.com/

CoinMarketCap, 2019. [Online] Available at: https://coinmarketcap.com/

Cointelegraph, 2018. [Online]. Available at: https://cointelegraph.com/news/eos-developer-acknowledges-claims-of-collusion-and-mutual-voting-between-nodes

Corbet, Shaen, Brian Lucey, Andrew Urquhart, and Larisa Yarovaya "Cryptocurrencies as a financial asset: A systematic analysis." *International Review of Financial Analysis* 62, 182-199, 2019.

Crain, Tyler, Vincent Gramoli, Mikel Larrea, and Michel Raynal. "DBFT: Efficient Leaderless Byzantine Consensus and its Application to Blockchains." *In 2018 IEEE 17th International Symposium on Network Computing and Applications* (NCA), pp. 1-8. IEEE, 2018.

Crain, Tyler, Vincent Gramoli, Mikel Larrea, and Michel Raynal. "DBFT: Efficient byzantine consensus with a weak coordinator and its application to consortium blockchains." 2017.

Croman, Kyle, Christian Decker, Ittay Eyal, Adem Efe Gencer, Ari Juels, Ahmed Kosba, Andrew Miller, Shi Saxena, EG Sirer, D. Song. "On scaling decentralized blockchains," in *International Conference on Financial Cryptography and Data Security*. Berlin and Heidelberg, Germany: Springer, 2016.

Dash, *Dash: A Payments-focused cryptocurrency,* 2019. [Online]. Available at: https://github.com/dashpay/dash/wiki/Whitepaper

Davidson, S., P. De Filippi, and J. Potts, “Blockchains and the economic institutions of capitalism,” *Journal of Institutional Economics*, *14*(4), pp.639-658, 2018.

Dierksmeier, Claus, and Peter Seele, "Cryptocurrencies and business ethics," Journal of Business Ethics 152, no. 1 (2018): 1-14, 2018.

Dinh, T.T.A., Liu, R., Zhang, M., Chen, G., Ooi, B.C. and Wang, J., “Untangling blockchain: A data processing view of blockchain systems,” IEEE Transactions on Knowledge and Data Engineering, 30(7), pp.1366-1385, 2018.

EOS Developer Guide, 2020. [Online] Available at: https://developers.eos.io/welcome/latest/protocol/consensus_protocol/

EOS.IO, *EOS.IO Technical White Paper*, 2019. [Online] Available at: https://github.com/EOSIO/Documentation/blob/master/TechnicalWhitePaper.md

Ethereum, *Ethereum 2.0 (Eth2)*, September 2020. [Online] Available at: https://ethereum.org/en/eth2/

Ethereum, *On sharding blockchain*, 2019. [Online] Available at: https://github.com/ethereum/wiki/wiki/Sharding-FAQ

Etherscan, 2019. [Online] Available at: https://etherscan.io

European Central Bank, *Virtual currency schemes*, October 2012. Available at: https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemes201210en.pdf

Evans, D., 'Economic Aspects of Bitcoin and Other Decentralized Public Ledger Currency Platforms.' Coase-Sandor Institute for Law and Economics Working Paper. No 685, 2014. Available at: http://www.law.uchicago.edu/Lawecon/index.htmlEuropean Central Bank, 2012

Evans, P, L. Aré, P. Forth, N. Harlé, and M. Portincaso, *A Strategic Perspective on Blockchain and Digital Tokens*. Boston Consulting Group, 2016. [Online]. Available: https://www.bcg.com/en-gb/publications/2016/blockchain-thinking-outside-the-blocks.aspx

Exaking, “PoW 51% Attack Cost,” 2019. [Online]. Available at: HTTPS://WWW.EXAKING.COM/51

Exaking, *PoW 51% Attack Cost*, 2019. [Online]. Available at: HTTPS://WWW.EXAKING.COM/51

Fani, Kees, Manuel Ferreira, and Cornel de Vroomen, *An Exploration of State-of-the-Art Blockchain Scalability Approaches*, 2019. [Online]. Available at: https://pdfs.semanticscholar.org/7cde/b2c8e132c2e003255d03dc3d14684831f894.pdf

Gervais, A., H. Ritzdorf, G. Karame, and S. Capkun, “Tampering with the delivery of blocks and transactions in bitcoin,” in *Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security*, pp. 692–705, 2015.

Gipp, B., N. Meuschke, and A. Gernandt. “Decentralized Trusted Timestamping using the Crypto Currency Bitcoin.” In *Proceedings of the iConference, 2015* (to appear), Newport Beach, CA, USA, Mar. 24 - 27, 2015. URL http://ischools.org/the-iconference/.

Grayblock, Blockchain Scalability, 2018. [Online]. Available at: https://medium.com/coinmonks/blockchain-scaling-30c9e1b7db1b

Infosys, “Resilience in distributed systems,” 2019. [Online}. Available at: https://www.infosys.com/industries/financial-services/insights/Documents/resilience-distributed-systems.pdf

Investopedia, Scalability, 2020. [Online]. Available at: https://www.investopedia.com/terms/s/scalability.asp

Jelurida, *Ardor/Nxt whitepaper*, 2019 [Online]. Available at: https://www.jelurida.com/sites/default/files/JeluridaWhitepaper.pdf

Kewell, B., Adams, R. and Parry, G., “Blockchain for good?” *Strategic Change*, 26(5), pp.429-437, 2017.

Khan, M., and K. Salah, “IoT security: Review, blockchain solutions, and open challenges,” *Future Generation Computer Systems-the International Journal of Escience*, vol. 82, pp. 395–411, 2018.

Kogias, E. K., P. Jovanovic, N. Gailly, I. Khoffi, L. Gasser, and B. Ford,“Enhancing bitcoin security and performance with strong consistency via collective signing,” in *25th {USENIX} Security Symposium ({USENIX} Security 16)*, 2016.

Kokoris-Kogias, L., L. Gasser, I. Khoffi, P. Jovanovic, N. Gailly, and B. Ford, "Managing identities using blockchains and CoSi," In 9th Workshop on Hot Topics in Privacy Enhancing Technologies (HotPETs 2016), no. POST_TALK. 2016.

Li, J., D. Greenwood, and M. Kassem. “Blockchain in the built environment and construction industry: A systematic review, conceptual models and practical use cases”, *Automation in Construction*, *102*, 288-307, 2017.

Li, M., J. Weng, A. Yang, W. Lu, Y. Zhang, L. Hou, L. Jia-Nan, Y. Xiang, and R. Deng, “Crowdbc: A blockchain-based decentralized framework for crowdsourcing,” *IEEE Transactions on Parallel and Distributed Systems*, *30*(6), pp. 1251-1266, 2017.

Li, X., P. Jiang, T. Chen, X. Luo, and Q. Wen, “A Survey on the Security of Blockchain Systems”, *Future Generation Computer Systems*, pp. 1-25, 2017.

Liquid, *What are the protocols in crypto and blockchain*, 2018. [Online] Available at: https://blog.liquid.com/what-are-protocols-and-why-are-they-important

Manoppo, *Blockchain Consensus Protocol “Trilemma” - Discussion & Analysis*, 2018. [Online]. Available: https://www.linkedin.com/pulse/blockchain-consensus-protocol-trilemma-discussion-analysis-manoppo

Mazieres, David, *The Stellar Consensus Protocol: A Federated Model for Internet-level Consensus*, 2016. [Online]. Available at: https://www.stellar.org/papers/stellar-consensus-protocol.pdf

Najjar, Walid, and J-L. Gaudiot, “Network resilience: A measure of network fault tolerance,” *IEEE Transactions on Computers* 39, no. 2, 174-181, 1990.

Nakamoto, S., *Bitcoin: A Peer-to-Peer Electronic Cash System*, 2008. [Online]. Assessed: https://bitcoin.org/bitcoin.pdf

NEO Developer Guide, 2020. [Online] Available at: https://docs.neo.org/developerguide/en/articles/blockchain/validator.html

Neo whitepaper, *Resources: NEO Basics/Consensus/Consensus Diagram*, 2019. [Online] Available at: https://docs.neo.org/docs/en-us/basic/whitepaper.html

NEO, 2019. [Online] Available at: https://neo.org/consensus

O'Dwyer, K. J., and D. Malone, D. "Bitcoin mining and its energy footprint." 25th IET Irish Signals & Systems Conference 2014 and 2014 China-Ireland International Conference on Information and Communications Technologies (ISSC 2014/CIICT 2014). 280 – 285.2014

Pereira, J., M. Tavalaei, and H. Özalp, "Blockchain-based platforms: Decentralized infrastructures and its boundary conditions", *Technological Forecasting and Social Change*, *146*, 94-102. 2019.

Raskin, Max, "Meet the Bitcoin Millionaires." Bloomberg Businessweek, April 10, 2013.

Risius, M., and K. Spohrer, "A blockchain research framework," *Business & Information Systems Engineering*, vol. 59, no. 6, pp. 385–409, 2017.

Romiti, M., A. Judmayer, A. Zamyatin, and B. Haslhofer, "A deep dive into bitcoin mining pools: An empirical analysis of mining shares," *arXiv preprint arXiv:1905.05999*, 2019.

Saad, M., J. Spaulding, L. Njilla, C. Kamhoua, S. Shetty, D. Nyang, and A. Mohaisen, "Exploring the Attack Surface of Blockchain: A Systematic Overview," 2019.Sherer, M. "Performance and Scalability of Blockchain Networks and Smart Contracts," 2017. [Online] Available at: http://www.diva-portal.org/smash/get/diva2:1111497/FULLTEXT01.pdf

Schroeder, Stan, *Bitcoin nears $10,000 as total value of all cryptocurrencies surpasses $300 billion*, 2019. [Online]. Available at: https://mashable.com/article/bitcoin-10000-2019/?europe=true.

Schwartz, David, Noah Youngs, Arthur Britto, *The Ripple Protocol consensus algorithm*, 2018. [Online] Available at: "https://ripple.com/files/ripple_consensus_whitepaper.pdf.

Stellarbeat.io, 2019. [Online] Available at: https://stellarbeat.io/

Vigna, P., and M. J. Casey. *Cryptocurrency: How Bitcoin and digital money are challenging the global economic order*. Random House, 2015. Available at: http://www.theinvestorspodcast.com/wp-content/uploads/2018/03/TheAgeofCryptoCurrency-NEW.pdf

Visa, *Stress test prepares visanet for the most wonderful time of the year*, 2019. [Online]. Available at: https://www.visa.com/ blogarchives/us/2013/10/10/stress-test-prepares-visanetfor-the-most-wonderful-time-of-the-year/index.html

Wang, W., D. T. Hoang, P. Hu, Z. Xiong, D. Niyato, P. Wang, Y. Wen, and D. I. Kim, "A survey on consensus mechanisms and mining strategy management in blockchain networks," *IEEE Access*, *7*, 22328-22370, 2019.

Wei-hong, H. U., A. O. Meng, S. H. I. Lin, X. I. E. Jia-gui, and L. I. U. Yang, "Review of blockchain-based DNS alternatives." *网络与信息安全学报* 3, no. 3: 71-77, 2017.

Williamson, O. E., "Transaction-cost economics: the governance of contractual relations," *The Journal of Law and Economics*, vol. 22, no. 2, pp. 233–261, 1979.

XRPcharts, 2019. [Online]. Available at: https://xrpcharts.ripple.com/#/validators

Zhang, S. and J. Lee. "Analysis of the main consensus protocols of Blockchain." ICT Express, 2019.