Decrypting Distributed Ledger Design - Taxonomy, Classification and Blockchain Community Evaluation

Mark C. Ballandies
Computational Social Science
ETH Zurich
Zurich, Switzerland
bmark@ethz.ch

Marcus M. Dapp
Computational Social Science
ETH Zurich
Zurich, Switzerland
mdapp@ethz.ch

Evangelos Pournaras
Computational Social Science
ETH Zurich
Zurich, Switzerland
epournaras@ethz.ch

***Abstract*—More than 1000 distributed ledger projects raising $600 billion in investments in 2016 feature the unprecedented and disruptive potential of the blockchain technology. A systematic analysis, comparison and rigorous evaluation of the different design features of distributed ledgers and their implications in performance and applications is a challenge. The fast evolving blockchain landscape creates an increasing gap in a common and comprehensive understanding of the techno-socio-economic design space of distributed ledgers and their supported crypto-economies. This paper contributes a conceptual architecture, a taxonomy and a classification of 29 distributed ledger systems. Compared to related work, the proposed taxonomy and classification is highly comprehensive and robust as defined in earlier taxonomy theory and validated in a crowd-sourced study using blockchain community feedback to harvest the wisdom of the crowd.**

I. Introduction

Over 1000 distributed ledger systems have emerged in the recent years raising investments of $600 billion in 2016 [1]. They empower a large spectrum of novel distributed applications using data immutability, integrity, fair access, transparency, non-repudiation of transactions [2] and crypto-currencies. These applications range from improving supply-chains [3], the creation of self-sovereign identities[1] [4], peer-to-peer energy markets [5], secure digital voting [6] to cross-country financial transactions [2]. The most well-known distributed ledger technology (DLT) is Bitcoin, whose novel consensus mechanism[2] and cryptoeconomic design[3] (CED) empowers untrusted parties to reach consensus [7]. Bitcoin is the first public distributed ledger system, which prevents double-spending[4] and sybill attacks[5] [8].

A *distributed ledger* (DL) is a distributed data structure, whose entries are written by the participants of a DLT system after reaching consensus on the validity of the entries. A *consensus mechanism* is usually an integral part of a distributed ledger system to guarantee system reliability: all written entries are validated without a trusted third party. Distributed ledgers are usually designed to support secure *cryptoeconomies* which are capable of operating cross-border, without depending on a certain political structure or legal system. These cryptoeconomies rely on digital currencies referred to as *tokens* and cryptographic techniques to regulate how value exchange is performed between the participating actors [9], [10]. The options and choices of a cryptoeconomy are referred to as *cryptoeconomic design* (CED) that plays a key role in the stability of a DLT system in terms of convergence, liveness and fairness [7].

Keeping up with the pace of this rapidly evolving technological landscape is a challenge. One reason is the lack of a common and insightful vocabulary that is earlier documented as a significant barrier [11]. Moreover, the plethora of design options for distributed ledgers and their supported cryptoeconomies have implications on performance and their applicability [2] that have neither been systematically studied nor rigorously formalized to guide researchers and practitioners to unravel new disruptive blockchain solutions [7], [12]. It has been argued that this can lead to fragmentation of the blockchain community and duplication of efforts [13]. The significance of this challenge is reflected on the recent taxonomies of distributed ledgers [2], [13], [14], [15].

In contrast to this earlier work, this paper introduces a conceptual architecture based on which a comprehensive and robust taxonomy is designed to classify 29 distributed ledger systems. A novel evaluation methodology is employed that engages the blockchain community and constructively uses its feedback to validate and improve further the proposed taxonomy and classification. In other words, the mapping of the blockchain landscape is crowd-sourced to the blockchain community itself to harvest the wisdom of the crowd.

The contributions of this paper are outlined as follows:

1) *A conceptual architecture* that models DLT systems into four components. The architecture defines a minimal and

[1]Decentralized identities, owned and controlled by the individual represented through the identity.

[2]Bitcoin uses a Nakamoto consensus, see Section IV-B.

[3]In particular, paying a block reward (Section IV-D) and transaction fees (Section IV-B) to its consensus participants.

[4]Faulty transactions of the same token to two different receivers

[5]Setup of fake identities to insert faulty information into the distributed ledger

insightful terminology to illustrate the inner mechanics of distributed ledgers and the interrelationships of their components.

2) *A taxonomy* of distributed ledgers that formalizes a set of 19 descriptive and qualitative attributes including a set of defined characteristics for each attribute. They illustrate in more detail the four DLT components (Figure 2) and provide deeper insights to cryptoeconomic terms, such as utility token, public blockchain, etc.
3) *A classification* of 29 DLT systems, including Bitcoin and Ethereum, which are backed up by an extensive literature review.
4) *A taxonomy evaluation criterion* referred to as 'expressiveness' designed from earlier theory on taxonomies.
5) *A crowd-sourced evaluation feedback* by blockchain community to further assess and improve the taxonomy and classification.

This paper is organized as follow: In Section II, terminology and recent taxonomies for DLT systems are discussed. A conceptual architecture for DLT systems is introduced in Section III, while a taxonomy in Section IV. Thereafter, Section V classifies 29 DLT systems based on the taxonomy. In Section VI, the community evaluation by blockchain practitioners is illustrated. Finally, in Section VII a conclusion is drawn and an outlook presented.

II. Background and Literature Review

DLT systems use different *types of distributed ledgers* as data structures. In particular, the literature distinguishes between distributed ledgers (DL) and blockchains [2], [12], the latter representing one way to implement the former. Another type of a distributed ledger is the directed acyclic graph [14].

The entries of a distributed ledger contain *transactions*. Any type of transaction can be stored, ranging from cryptographically signed financial transactions, to hashes of digital assets, and Turing complete executable programs [2]. DLT systems are able to define the *access rights to these transactions*: they determine who can initiate transactions, write them to the distributed ledger, and read them again from the ledger [2]. In addition, they use the so called *tokens* [15], which are identified as another key component of DLT systems, besides the distributed ledger [19]. Hence, these components can be modeled independently, resulting in systems, which do not necessarily maintain a native distributed ledger, but only define a token while using another system as their infrastructure for a distributed ledger. For instance, the Aragon system does not maintain a natively developed distributed ledger [20].

The capabilities to define the type of transactions, access rights and tokens, are used to influence user behavior, i.e. by limiting and granting access rights to system services or by incentivizing specific actions with tokens. These socio-economic choices not only influence system stability, such as correctness, liveness and fairness of the consensus mechanism [7], but also determine the emergence of complex cryptoeconomies [9], [10]. In other words, DLT systems reach stability and empower economies via their cryptoeconomic design (CED).

A DLT system has first to reach *consensus* before a transaction can be permanently written onto its ledger [15]. This consensus mechanism is a functional element of any DLT system [12], as it enables a decentralized network to unanimously take decisions about the validity of entries in the distributed ledger [21]. In particular, in the context of DLT systems, the consensus prevents double-spending of token units [22] and Sybill attacks [8] that are the setup of fake identities to inject faulty information into the distributed ledger.

Recent ontologies and taxonomies have been proposed to structure and map DLT systems. A comparative summary of earlier work is shown in Table I.

The criteira for the selection of the taxonomy attributes are not clearly determined. Only Paper 4 in Table I provides a conceptual framing (Column 3 in Table I), which motivates the choice of some attributes. More specifically, it distinguishes between on-chain and off-chain aspects [15]: components of the DLT system which exist on the distributed ledger (e.g. permission management) vs. components which exist outside (e.g. control, data).

The number of attributes across the papers varies considerably, from 4 to 30 attributes (Column 4 in Table I). One explanation is that the papers focus on different aspects of a DLT system and thus study different (sub) sets of attributes. For instance, Yeow et. al [14] (Paper 5 in Table I) focus on Internet of Things applications of DLT systems and only use four attributes, whereas Tasca et. al (Paper 1 in Table I) design a taxonomy to model all types of DLT systems and hence use 30 attributes [13]. Several of the attributes potentially have conceptual overlaps that stem from the lack of a supported conceptual architecture.

Consensus is identified as a core feature of DLT systems [21] and as such it is incorporated in all papers of Table I. For this reason it is omitted from this table. Nevertheless, only three papers consider incentivization schemes, with which participation in the consensus mechanism is motivated (Column 5 in Table I).

Moreover, only Paper 3 and 5 distinguish different types of distributed ledgers (Column 6 in Table I). For instance, Xu. et al. differentiate between blockchains and directed acyclic graphs [2]. Nevertheless, some of the most recent contributions only include blockchain-type DLT systems [2], [13], [16].

Five papers include cryptoeconomic design in their taxonomy (Column 8 in Table I). In particular, four papers consider the access rights to transactions (Column 8 in Table I) that also plays a key role in cryptoeconomic design. Only Paper 1 includes tokens and their properties in its taxonomy (Column 9 in Table I).

Paper 5 in Table I illustrates the classification of 28 DLT systems based on a proposed taxonomy (Column 10 in Table I). The authors relied on three attributes: data structure, scalable consensus ledger and transaction model [14]. However, they have not introduced formal criteria for the selection of the 28 DLT systems.

How effective and useful a taxonomy is usually depends on qualitative criteria studied in taxonomy theory [23] as well

TABLE I
COMPERATIVE OVERVIEW OF EARLIER WORK OUTLINING THE LANDSCAPE OF DISTRIBUTED LEDGERS.

ID	Paper	Concept	Attributes	Consensus Incentivization	Diff. DL	CED	Access rights to transactions	Token properties	Classification	Community Evaluation
1	Tasca et. al (2017) [13]	-	30	yes	-	yes	yes	yes	-	-
2	Comuzzi et. al (2018) [16]	-	8	yes	-	yes	yes	-	-	-
3	Xu et. al (2017) [2]	-	13	-	yes	yes	yes	-	-	-
4	Xu et. al (2016) [15]	yes	7	-	-	yes	yes	-	-	-
5	Yeow et. al (2018) [14]	-	4	-	yes	-	-	-	yes	-
6	Okada et. al (2017) [17]	-	4	yes	-	yes	-	-	-	-
7	De Kruijff et. al (2017) [18]	-	6 (many)	-	-	-	-	-	-	-
	This paper	yes	19	yes	yes	yes	yes	yes	yes	yes

as on the expert's knowledge who is the one designing the taxonomy. Another approach is to study more quantitatively the quality of a taxonomy based on crowd-sourced community feedback and the wisdom of the crowd. This is particularly relevant in the case of DLT systems and the blockchain community. The latter is the one shaping the blockchain landscape and therefore harvesting feedback can provide invaluable new insights about the design of distributed ledgers. Such an endeavor has not been pursued so far as shown in Column 10 of Table I.

The most comprehensive taxonomy, introduced by Tasca et al. [13], is worth a brief discussion. This taxonomy for DLT systems consist of eight components having a total of 30 attributes. It includes CED with three components: Native currencies/tokenisation, identity management and charging as well as rewarding system. In particular, access rights to transactions and the properties of a token are discussed. Access rights to the consensus and its incentivization are also illustrated. Despite the extensive coverage of relevant concepts, this taxonomy lacks a conceptual architecture connecting the elements, e.g. no information is given how the eight components relate to each other. Moreover, it remains unclear based on which criteria the authors introduce these eight components and 30 attributes. In addition, the distinction of CED from DL is not explicitly made as well as which of the components concern on-chain and which off-chain aspects. More particularly, this taxonomy does not differentiate between different types of distributed ledgers. This limits the option of a more granular differentiation of distributed ledgers that is a quality indicator for taxonomies as shown in Section VI-D.

In summary, a few observations can be made about the current state of the art on DLT system taxonomies. First, they predominantly focus on the DL and consensus mechanisms, while largely neglecting cryptoeconomics and token design, despite their significant role on system stability [7]. Second, they are usually not based on a conceptual architecture from which to derive the interrelationships of the different components as well as better interpretations of the different design choices. Third, none of the papers, except one, classifies real world DLT systems. This is a missed opportunity to validate the classification capacity of any proposed taxonomy. Last but not least, none of the proposed taxonomies is systematically exposed to feedback from blockchain practitioners. This complementary external validation promises richer, more unbiased and applicable taxonomies, especially at this early stage of the rapidly evolving DLT domain.

This paper addresses all of the aforementioned limitations identified in literature and contributes a new expressive taxonomy, built on a solid conceptual architecture, assessed via classifications and validated by feedback from the blockchain community. In particular, the classification is a proof of concept for the applicability and effectiveness of the developed taxonomy, as it demonstrates the expressiveness[6] of the taxonomy to differentiate and classify DLT systems.

.

III. Conceptual Architecture

By studying 29 DLT systems that academic literature covered at time of writing this paper (c.f. Table IV), a conceptual architecture[7] is introduced in this section. The architecture contains a set of four key components, their interrelationships and embodiment into the distributed ledger design space. The architecture is depicted in Figure 1. The four components are illustrated in the rest of this section.

Action component. A human or machine actor performs an action in the real world (Arrow (A) in Figure 1), for example planting a tree or doing a monetary transaction. Here, at the border between real world and digital world, the action gets a digital representation, which is referred to as claim.

Consensus component. Claims are broadcast to all nodes in the network that can participate in the consensus mechanism (Arrow (B)). These nodes (referred to as miners in Bitcoin or minters in Peercoin) collect these claims for writing them to the distributed ledger.

Distributed ledger component. Only at this point, the actual distributed ledger (or blockchain in the case of blockchain-type DLT systems) comes into play. Participants of the consensus combine these claims to entries (referred to as blocks in Bitcoin) and write them to the distributed ledger (Arrow (C)). This representation of the claim on the distributed ledger is called a transaction. Transactions and objects existing on the distributed ledger are referred to as on-chain, in contrast to off-chain objects, existing on the consensus or action component.

[6]Expressiveness is formally defined in Section VI-D based on earlier taxonomy theory.

[7]ISO/IEC/IEEE 42010:2011 standard [24]

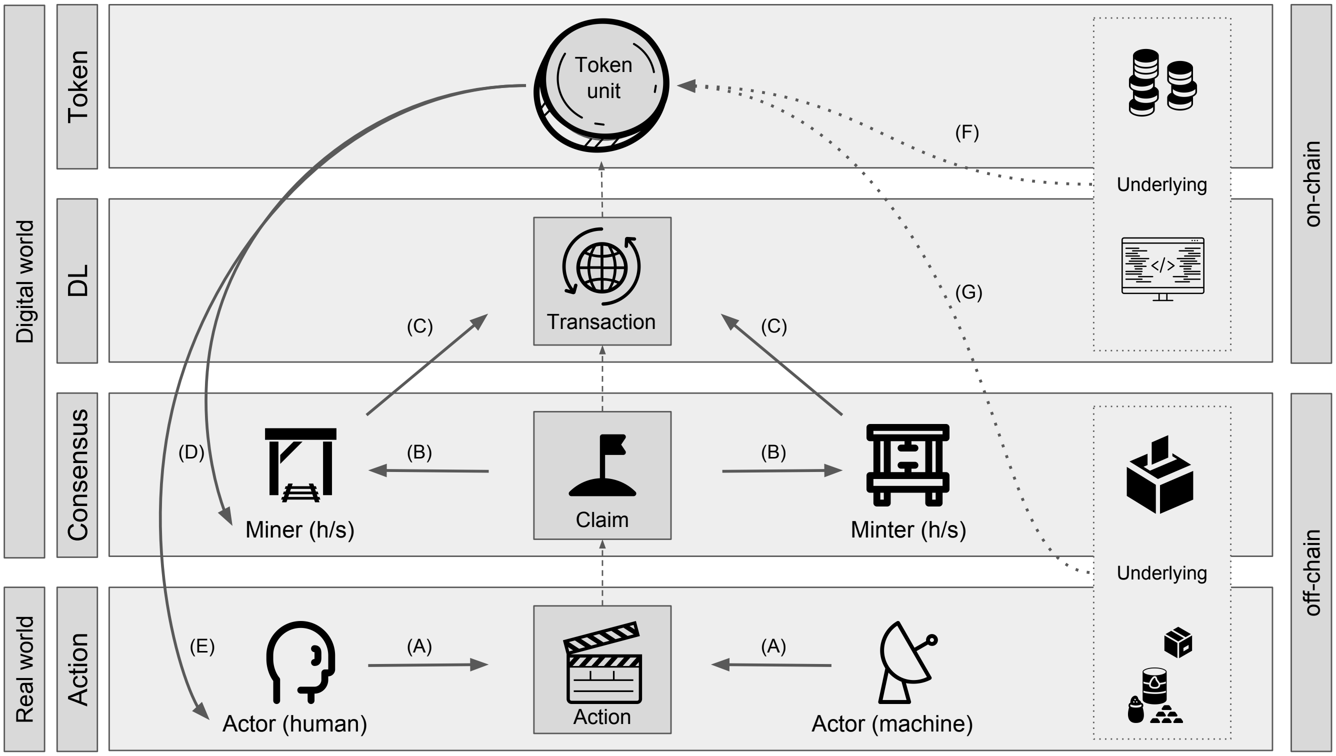


Fig. 1. An overview of the conceptual architecture with four key concepts of DLT systems and their relationship: action, consensus, distributed ledger and token.

Token component. Token creation depends on whether an incentive system is part of the DLT system. If it is, there are two options: token units are given as rewards to nodes, who are either involved in the consensus (Arrow (D)) or an action (Arrow (E)). While the inherent properties of such tokens (e.g. whether supply is capped or not) are determined by the design of the DLT system, the value given to token units is backed by underlyings, cryptoeconomic assets which can reside on-chain (Arrow (F), for example other tokens or executable code) or off-chain (Arrow (G), for example goods, services or commodities).

Example Ethereum. It is shown here how the identified components interact using a well-known DLT system. In Ethereum, one type of action is the deployment of a piece of code (Arrow (A) in Figure 1), a smart contract. These actions are collected by miners (Arrow (B)) and written as a block to the Ethereum distributed ledger (Arrow (C)). A miner, who successfully writes a block, obtains Ether, newly created token units as an incentive to mine (Arrow (D)). The Ether token has inherent properties, e.g. it has an uncapped supply. It also has value because it enables its owner to access the on-chain computational power of the Ethereum network (Arrow (F)).

IV. Taxonomy

Based on the conceptual architecture of Section III, a taxonomy is designed, using the method proposed by Nickerson et al. [23].

The taxonomy positions the four components of Section III across two dimensions to classify DLT systems (Figure 2). The first dimension concerns system design aspects related to the distributed ledger technology (DLT) – *distributed ledger component*, *consensus component* –, while the second concerns cryptoeconomic design aspects (CED) – *action component* and *Token component*.

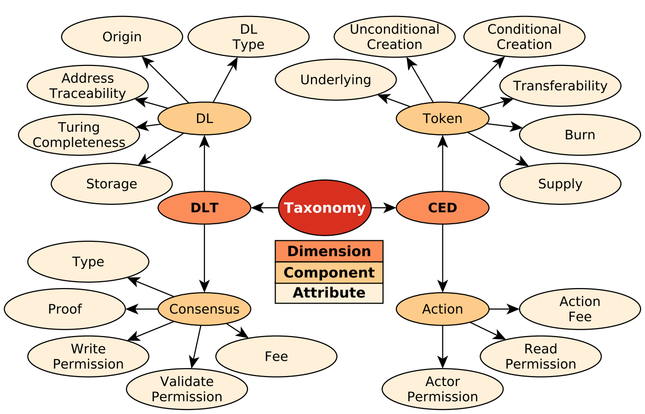


Fig. 2. Overview of the taxonomy, depicting the two dimensions of DLT and CED, its four components and 19 attributes.

A. Distributed Ledger

Definition 1. *A distributed ledger is defined as a distributed data structure, whose entries are digital records of actions.*

In the Bitcoin system, an entry in the data structure is called block. In the IOTA system, it is called bundle. An entry contains a set of transactions (Figure 1, distributed ledger component). In Bitcoin, these transactions represent exchange of currency value.

The attributes of the distributed ledger are *type*, *origin*, *address traceability* and *Turing completeness*.

1) Type: illustrates the data structure of the distributed ledger. Type has the characteristics *blockchain*, *directed acyclic graph* (DAG) or *other*.

The most well known type is the blockchain; an immutable and append-only linked list, which has a total order of elements. Several systems use blockchains, such as Bitcoin [2], Ethereum [25] or Litecoin [26].

In contrast to these systems, IOTA uses a directed acyclic graph [14]. This data structure is no longer a linked list, but a directed graph with no cycles, leading to a partial order of elements. Moreover, Ripple neither uses a blockchain nor a directed acyclic graph, but operates on other consensus based accounting mechanism [27].

2) Origin: defines the ownership of the distributed ledger. It has the characteristic *native*, if the distributed ledger is maintained by and for the system itself or *external*, if the system uses a distributed ledger from another DLT system.

The level of ownership varies between the different DLT systems. Bitcoin develops and maintains its distributed ledger natively, likewise NXT [15]. In contrast, Aragon [20], Augur [28] [27] and Counterparty [14] do not maintain a native distributed ledger, they use Ethereum or Bitcoin as an infrastructure. Systems can use a hybrid approach. Factom combines a natively developed concept of a blockchain and its own consensus mechanism with the Bitcoin blockchain [2].

3) Address traceability: shows the extent to which different transactions, originating from or incoming at the same chain identity, can be linked together. It has the characteristic *obfuscatable*, if the distributed ledger has mechanisms in place to hide such links and *linkable* if links can be inferred with some computational effort.

The level of address traceability varies between the different DLT systems. Zcash [2] and Monero [13] are so called privacy coins, which perform advanced measures to unlink transactions [7]. Hence, the on-chain identities of the actors remain obfuscated. Bitcoin has a linkable address traceability [29]. In theory, transactions cannot be linked to a chain identity, but it is shown, that with some computational effort this can be actually achieved [2]. The same linkability property holds for Ripple [30].

4) Turing completeness: determines whether a Turing machine can be simulated by the DL. It has the characteristic *Yes* or *No*.

Some DLs can execute Turing machines. Ethereum is an example of these. It allows for the storage and execution of Turing complete smart contracts [15], in contrast to the Bitcoin blockchain [29].

5) Storage: determines if additional data can be stored on the distributed ledger besides default transaction information.

The characteristics are *yes*, if data can be stored and *no*, if no additional data can be stored.

The distributed ledger of Bitcoin allows for the storage of arbitrary data inside of transactions. This allows Bitcoin to be used as a first layer system, see Section IV-E, which is done by Counterparty [14]. In contrast to Bitcoin, IOTA does not allow for such an additional storage of data [31].

B. Consensus

Definition 2. *Consensus is the mechanism of writing entries to the distributed ledger, adhering to a set of rules that all participants of the consensus enforce when an entry containing transactions is validated.*

The attributes of consensus are *type*, *proof*, *write permission*, *validator permission* and *fee*.

1) Type: shows whether the consensus is deterministic or probabilistic. Hence, its characteristics are: *deterministic*, if consensus is found in guaranteed finite amount of time or *probabilistic*, if consensus is found with some uncertainty.

Most DLT systems use the Nakamoto consensus [2], a Byzantine Fault Tolerance (BFT) algorithm. This type of algorithms tolerate a class of system failures that belong to the Byzantine Generals Problem[32]. In particular, a consensus algorithm having this property prevents consensus participants to write a false transaction to the distributed ledger.

In contrast to other BFT algorithms, the Nakamoto consensus is probabilistic. This type of algorithm validates a new entry by utilizing the whole history of previous entries: An entry is accepted as confirmed if and only if there is a certain number of new entries referencing it [7]. For instance, in Bitcoin, a writer validates a transaction by considering the whole blockchain and includes then the transaction into a new block. As soon as this block gets referenced by six blocks, it is confirmed, as the probability that a second chain of six blocks referencing each other, but not referencing this block, is low [2]. Likewise, in the directed acyclic graph of IOTA an entry is confirmed, when it is referenced by a significant number of new entries [14]. On the other hand, Ripple does not use a Nakamoto consensus for its algorithm. Its consensus is found in guaranteed finite amount of time [21].

2) Proof: is the evidence with which a consensus is found. It has the characteristics: *proof-of-work* (PoW), if it is delivered by utilizing processing power of computers; *proof-of-stake* (PoS), if it is delivered by voting linked to (economic) power in the system; *hybrid*, if it is a combination of the previous two or *other*, if another form of proof is required.

The proof is required by the consensus participants to accept the validity of an entry. Bitcoin uses a proof-of-work [15], which is the solution to a mathematical puzzle requiring the processing power of computers. A proof-of-stake is used by Ardor [13], which is the signature of a randomly selected consensus participant requiring the participant to hold a stake in Ardor token units.

3) Write permission: illustrates who is allowed to write entries to the distributed ledger. The characteristics are *restricted*, if participation is restricted or *public* otherwise.

The Bitcoin consensus mechanism is public [15], it allows everyone having computing power to participate [21]. On the other hand, the consensus mechanism of Ripple is restricted [15], it has a few trusted institutions, which perform consensus, and hence not everyone can participate [14].

4) Validate permission: shows who is allowed to validate claims before they are written to the distributed ledger. The characteristics are: *restricted*, if participation is restricted and *public* otherwise.

In Bitcoin, the writers validate claims for correctness, utilizing the proof, before they write them to a block, hence the validator permission is also public. In contrast, in IOTA a central entity, the coordinator, validates transactions before they are collected in an entry and written to the directed acyclic graph [14].

5) Fee: shows whether participants of the consensus (writers and validators) are paid a fee for writing new entries to the distributed ledger. The characteristics are *yes* and *no*.

In contrast to Bitcoin, where writers/ validators are rewarded with fees [21], in IOTA the writers and validators receive no fees [14]. In Ripple no fees are rewarded to the consensus participants, although the actors have to pay a fee [33].

C. Action

Definition 3. *An action is one or more real-life activities, which can be digitally represented by a DLT system as a transaction.*

In this sense, a transaction represents digitally a real-life action. The attributes of action are *actor permission*, *read permission* and *fee*.

1) Actor permission: illustrates who can perform an action.

The characteristics are *restricted*, if actors have to fulfill special requirements before performing actions in these systems or *public*, if anyone can perform actions.

Bitcoin allows everyone to create a private key to send/ receive token units [13], hence it has a public actor permission. Ripple uses restricted access rights. In order to comply with regulations (e.g. know-your-customer), actors need to register [13].

2) Read permission: illustrates the scope of actors who can read contents of transactions from the distributed ledger.

The characteristics are: *restricted*, if permission is preconditioned, or *public*, if permission is not restricted.

Most DLT systems have a public read access in the sense that everyone can read the content of occurred actions, e.g. the amount of transferred bitcoins [13]. Privacy coins often restrict read access to actors of the transaction (e.g. Zcash [2]), usually by making an effort to hide the amount of transfered token units [7].

3) Fee: shows whether the actor has to pay a fee for performing an action that is not related to the consensus. The characteristics are *yes* or *no*.

Some DLT systems require actors to pay a consensus-independent fee, before they can store an action on the distributed ledger. For instance, actors have to pay a fee in Augur, which is not paid to the consensus participants [28]. In Bitcoin no additional fee is required to perform an action, except the one paid to the consensus participants. Also Ripple requires actors to pay a fee per action, which is not paid to consensus participants, but is destroyed [33].

D. Token

Definition 4. *Token is a unit of value issued within a DLT system and which can be used as a medium of exchange or unit of account.*

Its attributes are *supply property*, *burn property*, *conditional creation*, *unconditional creation*, *onchain underlying*, *offchain underlying*.

1) Supply property: illustrates the total quantity of token units made available. The characteristics are *capped*, if the total supply is bound by a finite number and *uncapped* otherwise.

Under increasing demand for a currency, a capped supply can result in an appreciation of the currency and to a deflation of prices denominated in it. Moreover, it can result in an appreciated exchange rate with other currencies, which in turn increase the stability of a DLT system [7]. Bitcoin has a capped supply of 21 million units [13], whereas Dodgecoin does not have an upper limit [29].

2) Burn property: illustrates whether token supply is reduced by removing token units. The characteristics are *yes* or *no*.

Some DLT systems destroy token units that is a processed referred to as 'burn'. This decrease in money supply, while observing a constant demand results in an appreciation of the token units and hence, a better exchange rate with other currencies. For example in Ripple, paid fees are removed from the total supply and are not returned [33]. In contrast, Bitcoin has no inherent destruction mechanism of its token units.

3) Transferability: determines, if the ownership of a token unit can be changed. The characteristics are *transferable*, if the token can be transfered and *non-transferable* otherwise.

Bitcoin token units can be transfered between different actors. Akasha plans to use non-transferable reputation tokens, so called Mana and Essence [34].

4) Conditional creation: illustrates how the creation of new token units is bound to incentivize the consensus and/ or an action. The characteristics are: *consensus*, if creation is bound to the consensus, *action*, if the creation is bound to an action, *both*, if the creation is bound to the consensus as well as the action and *none* otherwise.

In Bitcoin, new tokens are created by incentivizing the consensus mechanism [2]. Other systems create new tokens by incentivizing an action. For instance, in Steemit new steem is created by incentivizing content creation on the platform (e.g. writing blog articles) [35]. Moreover, Ripple does not use its token to incentivize the consensus or an action [36]. Furthermore, hybrid versions are possible, where new tokens are created by incentivizing the consensus and an action. For instance, newly created token units in the DASH system are awarded both to the consensus participants and the master nodes, which perform actions such as mixing transactions to enable an obfuscatable address traceability [37].

5) Unconditional creation: illustrates the amount of new token units that are created independent of incentivizing the consensus or an action. The characteristics are *partially*, if some tokens are created independently, *all*, if all tokens are created independently (e.g. 100 % pre-mined tokens) or *none* otherwise.

At genesis of the Bitcoin system, no token units are previously mined and all tokens come into existence by incentivizing the consensus [7] (characteristic: none). On the other hand, all Ripple tokens are created during the genesis of the system (characteristic: all). In Augur, some tokens are created during the genesis of the system [28] (characteristic: partially).

6) Underlying: illustrates where the source of value lies and what it constitutes of.

The characteristics are *distributed ledger*, if the token gives access to the distributed ledger, e.g. if the token is needed in order to use the storage or computing capacity of the distributed ledger; *consensus*, if the token gives access to the consensus mechanism, e.g. proof-of-stake; *action*, if the token gives access to perform or receive actions or services in the DLT system; *token*, if the token gives access to another token; *physical asset*, if the token gives access to goods or commodities external to the DLT system; *none*, if the token has no underlying.

The first two characteristics (distributed ledger and token) are considered to be on-chain and the other three are considered to be off-chain underlyings of a token unit (as depicted in Figure 1).

The Ethereum token allows everyone to store data or smart-contracts on-chain [2] and to access in this way the distributed ledger of the network. Hence Ether token units give access to the processing power of the distributed ledger, which gives value to the token units. In contrast to Ether, the Golem network token units allow holders to access off-chain computations [27]. Thus its underlying is an action as the token gives access to computing actions in the DLT System. The Storj Token allows users to access off-chain storage [13] and hence to perform a storage action. Siacoin allows for the storage of arbitrary data on both its distributed ledger [38] and its off-chain network [39]. Hence its underlying is the distributed ledger and action.

E. Cryptoeconomic Reasoning using Boolean Algebra

The introduced taxonomy allows for a more systematic definition of widely used yet not clearly defined terms in the field of DLT systems by combining specific taxonomy attribute characteristics with operators from boolean algebra. As illustrated in Table II, one can reason about terms such as permissioned/ permissionless blockchains, as well as asset/ utility tokens.

TABLE II
FORMAL DEFINITIONS ABOUT DLT SYSTEMS BY REASONING USING BOOLEAN ALGEBRA AND THE PROPOSED TAXONOMY.

System Term	**Formal Definition**
Blockchain	*blockchain* type
1st layer	*native* ownership
2nd layer	*external* ownership
Permissioned	*restricted* write permission OR *restricted* validator permission
Permissionless	*public* write permission AND *public* validator permission
Public	⟨*permissionless DLT system*⟩ AND *public* actor permission
Private	⟨*permissioned DLT system*⟩ AND *restricted* actor permission
Privacy	*obfuscatable* traceability AND ⟨*public DLT System*⟩
Infrastructure	*yes* turing completeness OR *yes* storage
Blockchain-as-a-Service	$\nexists$ action component attribute AND $\nexists$ token component attribute
Cryptoeconomic Term	
Utility	*distributed ledger* underlying OR *action* underlying
Asset	*token* underlying OR *physical good* underlying
Payment	*yes* transferability

In particular, the latter pair has been identified by the swiss financial market supervisory authority FINMA as important for the decision if a token is classified as a security. Such a treatment is of interest for market participants, because it has regulatory implications [40].

V. CLASSIFICATION

Twenty-nine DLT systems are classified according to the introduced taxonomy. The criterion for the selection is, that they are cited in academic literature.

The classification is given for each of the four components separately in the next subsections. A summary can be found in Tables III, IV, V, VI. The entries, i.e. attribute values, of the tables are accompanied with citations, if they are justified in academic literature. At least one entry per system is referenced in literature that is the criterion for the inclusion of a DLT system. All other information is derived from the DLT systems whitepapers or other web sources, such as the DLT system websites. All DLT system websites are cited in the second column of each of the Tables III, IV, V, VI.

A. Distributed Ledger

Table III shows 29 DLT systems classified according to the attributes of the distributed ledger component. Seven systems

TABLE III
SYSTEMS CLASSIFICATION ACCORDING TO THE DISTRIBUTED-LEDGER COMPONENT

ID	DLT System	Origin	Type	Address Traceability	Turing Completeness	Storage
1	Aragon [41]	External (Ethereum) [20]	-	-	-	-
2	Ripple [42]	Native [7]	Other [27]	Linkable [30]	No	Yes
3	Peercoin [43]	Native [13]	Blockchain [14]	linkable	No	Yes
4	Monero [44]	Native [13]	Blockchain [25]	Obfuscatable [13]	No	Yes
5	Hyperledger (Fabric) [45]	Native [14]	Other	Linkable [21]	Yes [14], [21]	Yes
6	Dash [46]	Native [13]	Blockchain [25]	Obfuscatable	No	Yes
7	Augur [47]	External (Ethereum) [28] [27]	-	-	-	-
8	Dogecoin [48]	Native	Blockchain	Linkable	No	Yes
9	Zcash [49]	Native	Blockchain [25]	Obfuscatable [2] [50]	No	Yes
10	EOS [51]	Native	Blockchain	Linkable	Yes	Yes
11	Byteball [52]	Native [14]	DAG [14]	Obfuscatable	No	Yes
12	Golem [53]	External (Ethereum)	-	-	-	-
13	Stellar [54]	Native [14]	Other	Linkable	No	Yes
14	Factom [55]	Hybrid (Bitcoin) [15] [2]	Blockchain	Linkable	No	Yes
15	Namecoin [56]	Native	Blockchain	Linkable	No	Yes
16	Omni [57]	External (Bitcoin) [15]	-	-	-	-
17	Storj [58]	External (Ethereum)	-	-	-	-
18	Sia [59]	Native	Blockchain	Linkable	No	Yes
19	SafeNetwork [60]	Native	Other	Linkable	Yes	Yes
20	Blockstack Core [61]	Hybrid (Bitcoin)	Blockchain	Linkable	No	Yes
21	Filecoin [62]	Native	Blockchain	Linkable	Yes	Yes
22	Ethereum [63]	Native [15]	Blockchain [25]	Linkable	Yes [7] [25]	Yes
23	Corda [64]	Native	Other	Obfuscatable	Yes [21]	Yes
24	Counterparty [65]	External (Bitcoin) [7] [14]	-	-	-	-
25	Enigma [66]	External (Ethereum)	-	-	-	-
26	IOTA [67]	Native	DAG	Linkable	No [14]	No
27	Litecoin [68]	Native [13]	Blockchain [25] [26]	Linkable	No	Yes
28	Bitcoin [69]	Native	Blockchain [2] [12]	Linkable [7] [13]	No [15] [7]	Yes
29	Ardor [70]	Native	Blockchain	Linkable	No	Yes

do not maintain their own DL. Hence the attributes type, read permission, address traceability and turing completeness are not specified for these, as the characteristics can be determined from the DL of the infrastructure[8] system.

Fifteen systems use a blockchain, two systems use a directed acyclic graph and five systems use another type of consensus based accounting mechanism. All 2nd layer systems as defined in Table II use a blockchain type system as an infrastructure. This is possibly because both, the first DLT system (Bitcoin) and the most widely-used DLT system that supports Turing complete smart contracts (Ethereum), are blockchain type systems [2] [15].

Seventeen distributed ledgers are linkable. These are systems which do not hide interactions of actors on the distributed ledger. DLT systems focusing on privacy, such as Zcash (System 7 in Table III), hide interactions between nodes with public addresses. Hence they allow their actors an anonymous participation, if they combine it with a public actor permission (see Section V-C). Some DLs allow to store and execute Turing complete code. Ethereum (System 22 in Table III) is the most widely used system enabling this [2]. In total there are six DLT systems in the classification having a Turing complete distributed ledger. Three of these are Blockchain systems and three are classified as other. No Turing complete directed acyclic graph has been identified among these DLT systems. All systems, except for IOTA, allow the storing of additional data on the distributed ledger. For instance, this enables Bitcoin to function as an infrastructure blockchain for systems such as Counterparty.

[8]Refer to Table II for a definition of infrastructure DLT system

B. Consensus

Table IV depicts the classification of the systems according to the consensus component. Systems, which do not maintain their own DL, do not also maintain a consensus mechanism, and hence have no attributes specified.

TABLE IV
SYSTEMS CLASSIFICATION ACCORDING TO THE CONSENSUS COMPONENT

ID	DLT System	Consensus Type	Proof	Write Permission	Validator Permission	Fee
1	Aragon [41]	-	-	-	-	-
2	Ripple [42]	Deterministic [21] [15]	Other	Restricted [2] [14]	Restricted	No
3	Peercoin [43]	Probabilistic	Hybrid [13], [14]	Public [14]	Public	No
4	Monero [44]	Probabilistic	PoW	Public	Public	Yes
5	Hyperledger (Fabric) [45]	Deterministic [13] [14]	Other	Restricted [71], [72]	Restricted	No
6	Dash [46]	Probabilistic	PoW	Public	Public	Yes
7	Augur [47]	-	-	-	-	-
8	Dogecoin [48]	Probabilistic	PoW	Public	Public	Yes
9	Zcash [49]	Probabilistic	PoW	Public	Public	Yes
10	EOS [51]	Deterministic [73]	PoS [73]	Restricted	Restricted	No
11	Byteball [52]	Deterministic [14]	Other [14]	Public	Restricted	Yes [14]
12	Golem [53]	-	-	-	-	-
13	Stellar [54]	Deterministic [2], [21]	Other	Restricted [13] [14]	Restricted	No
14	Factom [55]	Probabilistic	Other	Restricted	Restricted	No
15	Namecoin [56]	Probabilistic	PoW	Public	Public	Yes
16	Omni [57]	-	-	-	-	-
17	Storj [58]	-	-	-	-	-
18	Sia [59]	Probabilistic	PoW	Public	Public	Yes
19	SafeNetwork [60]	Deterministic	Other	Restricted	Restricted	No
20	Blockstack Core [61]	Probabilistic	Other	Unkown	Unkown	Unkown
21	Filecoin [62]	Probabilistic	Other	Public	Public	Yes
22	Ethereum [63]	Probabilistic	PoW [2] [14]	Public [15] [14]	Public	Yes [15]
23	Corda [64]	Deterministic	Other	Restricted	Restricted	No
24	Counterparty [65]	-	-	-	-	-
25	Enigma [66]	-	-	-	-	-
26	IOTA [67]	Probabilistic [14]	PoW [14]	Public [14]	Restricted	No [14]
27	Litecoin [68]	Probabilistic	PoW	Public	Public	Yes
28	Bitcoin [69]	Probabilistic [7] [2]	PoW [15] [21]	Public [15] [21]	Public	Yes [15] [21]
29	Ardor [70]	Probabilistic	PoS	Public	Public	yes

It is observed, that all permissionless systems use a probabilistic consensus. On the other hand, systems which have a restricted write and/or validate permission (permissioned system) and hence use a limited set of trusted third parties in their system, usually adopt a deterministic consensus (except System 14 and 26 in Table IV).

Both systems using a directed acyclic graph have a restricted validate permission. A permissionless directed acyclic graph is not apparent in literature during the writing of this paper.

All permissionless systems use consensus related fees. These are used to incentivize the writers and validators to participate in the consensus. Permissioned systems with the exception of one, Byteball (System 12 in Table IV), do not utilize consensus related fees. This is because these systems do not rely on anonymous participants for their consensus mechanism, but on trusted third parties.

C. Action

In Table V the classification of the systems for the action component is depicted. Two systems are blockchain-as-a-service, which provide distributed ledger services for other systems, but do not maintain a live instance of a distributed ledger. Thus, these systems do not deal with cryptoeconomic design decisions and hence have no specification for these attributes of the action component.

All other systems, except for two, have a public actor permission. For instance, Ripple does not provide everyone with system access, as it complies with Know-your-Customer regulations [13].

Systems with a focus on privacy usually restrict the read access of the transactions content hence (partially) restrict the access for third-parties to knowing what actions are performed by other actors.

TABLE V
SYSTEMS CLASSIFICATION ACCORDING TO THE ACTION COMPONENT

ID	DLT System	Actor Permission	Read Permission	Action Fee
1	Aragon [41]	Public	Public	Yes
2	Ripple [42]	Restricted [13]	Restricted [13]	Yes
3	Peercoin [43]	Public	Public	Yes [13]
4	Monero [44]	Public	Restricted	No
5	Hyper. (F.) [45]	-	Restricted [21]	-
6	Dash [46]	Public	Public	Yes
7	Augur [47]	Public [28]	Public	Yes [28]
8	Dogecoin [48]	Public	Public	No
9	Zcash [49]	Public	Restricted [2]	No
10	EOS [51]	Public	Restricted	No [73]
11	Byteball [52]	Public	Restricted	No
12	Golem [53]	Public	Public	Yes
13	Stellar [54]	Restricted [13]	Public	Yes [13]
14	Factom [55]	Public	Public	Yes
15	Namecoin [56]	Public	Public	No
16	Omni [57]	Public	Public	Yes
17	Storj [58]	Public	Public	Yes
18	Sia [59]	Public	Public	Yes
19	SafeNetwork [60]	Public	Public	No
20	Blockstack C. [61]	Public	Public	Yes
21	Filecoin [62]	Public	Public	Yes
22	Ethereum [63]	Public	Public	No
23	Corda [64]	-	Restricted	-
24	Counterparty [65]	Public	Public	Yes
25	Enigma [66]	Public	Restricted [13]	Yes [15]
26	IOTA [67]	Public	Public	No
27	Litecoin [68]	Public	Public	No
28	Bitcoin [69]	Public [13]	Public [13]	No
29	Ardor [70]	Public	Public	No

Fourteen systems require actors to pay an unrelated consensus fee for performing actions, i.e. Ripple (System 2 in Table V). It burns the fees as a spam protection, whereas Aragon (System 1 in Table V) collects fees from its network participants to maintain the network. These fees are not rewarded to participants of the consensus mechanism.

D. Token

Table VI depicts the classification for the token component. In case a system uses several tokens in its CED, only the main token for the operation of the system is classified.

Two systems do not have their own token. These are blockchain-as-a-service systems, which do not deal with cryptoeconomic design, but allow their users to define their own tokens on top of their distributed ledger (see Figure 1).

Seventeen systems capped the supply of token units to a finite number. Seven systems have an inherent burn mechanism implemented in their token. All of the classified tokens are transferable. In non academic literature the concept of non transferability is already discussed: Akasha plans to use non transferable reputation tokens, the so called Mana and Essence [34].

Fifteen systems incentivize participants of the consensus via rewarding them with newly mined token units of the system. All except one are blockchain based systems (System 19 in Table IV), only two of them use a deterministic consensus mechanism (System 10 and 19 in Table IV) and three of them are permissioned systems (System 10, 14 and 19 in Table IV).

Seven systems create new token units to incentivize an action. All of these systems are either a 1st layer DLT system as defined in Table II with a distributed ledger of type blockchain or use such a blockchain type system as an infrastructure. Nine systems bind the creation of new token units exclusively to incentivize an action or consensus. All of these systems are blockchain based systems. Ten systems create some token units unconditionally and eight systems create all units unconditionally. Only half of those that create all token units unconditionally are blockchain based, despite making up 75% of the overall classified systems.

This paper identifies two mechanisms to incentivize participation in the consensus mechanism: Consensus related transaction fees and block rewards, namely awarding token units to consensus participants. Bitcoin was the first DLT system to enable reaching consensus between untrusted parties [7] using both of these incentive mechanisms. This has influenced further developments in the field and hence, only two of the permissionless systems differ from this approach. All systems which use both incentive mechanisms are permissionless blockchain systems.

Eighteen tokens give access to the distributed ledger, seventeen tokens give access to actions and two tokens give access to the consensus of the DLT system. One token does not give access to any underlying.

VI. EVALUATION

The taxonomy (Section IV) and the classification of the initial set of DLT systems (Section V) is evaluated by feedback from the blockchain community. Participants were identified via their contributions to Github[9] repositories of DLT systems and their official websites. Participants received a personalized email invitation to a scientific survey with both a classification of their own DLT system and the taxonomy. A total of 209 invitations were sent out from which 56 practitioners in the field responded (response rate 26.8%). Thirty-six of those finished the survey (17.2%). The responses were collected during a period of three month, starting from the 22nd of March 2018.

The feedback resulted in adjustments of the classification and taxonomy that are illustrated in Section VI-C. The original version can be found in the supplementary material. The rationale behind the incorporation of the community feedback is explained in the following sections and in the supplementary material.

[9] Available at https://github.com (last accessed: October 2018).

TABLE VI
SYSTEMS CLASSIFICATION ACCORDING TO THE TOKEN COMPONENT

ID	DLT System	Token Name	Supply Property	Burn Property	Transferability	Conditional Creation	Unconditional Creation	Underlying
1	Aragon [41]	ANT	Capped	Yes	Transferable	Action	Partially	Action [20]
2	Ripple [42]	Ripple	Capped	Yes	Transferable	None	All	DL, Action
3	Peercoin [43]	Peercoin	Uncapped	Yes	Transferable	Consensus	None	DL, Consensus
4	Monero [44]	Monero	Uncapped	No	Transferable	Consensus	None	DL
5	Hyperledger (F.) [45]	-	-	-	-	-	-	-
6	Dash [46]	Dash	Capped	No	Transferable	Both	None	DL, Action
7	Augur [47]	Reputation	Capped	No	Transferable	Action [28]	Partially [28]	Action [28]
8	Dogecoin [48]	Dodgecoin	Uncapped [13]	No	Transferable	Consensus	None	DL
9	Zcash [49]	Zcash	Capped	No	Transferable	Consensus	Partially	DL
10	EOS [51]	EOS	Uncapped	No	Transferable	Consensus	Partially	DL [73]
11	Byteball [52]	GByte	Capped [14]	No	Transferable	None	All	DL
12	Golem [53]	GNT	Capped	No	Transferable	None	All	Action [27]
13	Stellar [54]	Lumen	Uncapped	No	Ttransferable	None	All	DL, Action
14	Factom [55]	Factoids	Uncapped	Yes	Transferable	Consensus	Partially	DL, Action [15]
15	Namecoin [56]	Namecoin	Capped	Yes	Transferable	Consensus	None	DL, Action [7] [74]
16	Omni [57]	Omni	Capped	Yes	Transferable	Action	None	Action
17	Storj [58]	Storj	Capped	No	Transferable	None	All	Action [71] [74]
18	Sia [59]	Siacoin	Uncapped	Yes	Transferable	Consensus	Partially	DL, Action [39] [74]
19	SafeNetwork [60]	SafeCoin	Capped	Yes	Transferable	Consensus	Partially	Action [74]
20	Blockstack C. [61]	Stacks	Uncapped	No	Transferable	Both	Partially	DL, Action [71] [74]
21	Filecoin [62]	Filecoin	Capped	No	Transferable	Both	Partially	DL, Action [71] [74]
22	Ethereum [63]	Ether	Uncapped	No	Transferable	Consensus [25]	Partially	DL [25] [75]
23	Corda [64]	-	-	-	-	-	-	-
24	Counterparty [65]	Counterparty	Capped	Yes	Transferable	Action [2] [15]	None	Action
25	Enigma [66]	Enigma	Capped	No	Transferable	None	All	Action [71] [76]
26	IOTA [67]	MIOTA	Capped [14]	No	Transferable	None	All	None
27	Litecoin [68]	Litecoin	Capped	No	Transferable	Consensus	None	DL
28	Bitcoin [69]	Bitcoin	Capped [7] [13]	No	Transferable	Consensus [7] [21]	None	DL [2]
29	Ardor [70]	Ardor	Capped	No	Transferable	None	All	DL, Consensus

The survey is divided into two parts. The first part lets participants evaluate the classification of their system while the second part acquires feedback on the structure of the taxonomy.

A. Demographics

Table VII illustrates the demographics of the survey, in particular, the distribution of participants among the DLT systems, their specific roles and experience. It shows that the participants are involved in 19 out of the 29 systems of the classification. Twelve developers participated in the survey of which 7 are core/team developers. Additionally 9 participants are project leaders. Moreover, 14 participants have more experience than three years, 16 participants work one to three years and 6 participants work shorter than a year in the field of DLT systems.

B. Classification

In the first part of the survey, the participants are shown the classification of their DLT system for 18 attributes of the four components. Consult Figure 2 for an overview of attributes[10] and Tables III, IV, V, VI for the rated classifications.

The participants have the option to agree, disagree or state that they are uncertain about the classification. They always have the chance to comment on their decision, irrespective of their choice.

Figure 3(a) depicts the aggregated rating of the components. The distributed ledger component has the highest approval with 90.5%, followed by action (85.6%), consensus (80.6%) and token (77.2%).

In the original version of the classification received by participants and illustrated in the Supplementary Material, the underlying attribute is split into on-chain and off-chain underlying. These attributes have more fine grained characteristics (e.g. Computation, Storage, Identity) than the one used in the final classification as explained in Section VI-C.

Figure 4 shows the approval ratings for each attribute of the four components. One notices, that all approval ratings are above 74%, except on-chain underlying (50.0%) and off-

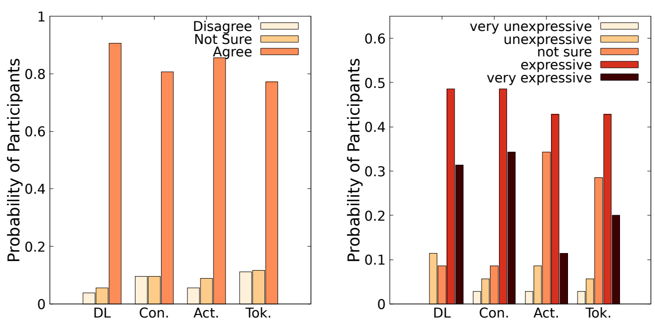
[10]Please note, that the number of attributes presented to the survey participants differ from the final number of attributes. The reasoning for this is explained at the end of this Section

TABLE VII
SURVEY PARTICIPANTS PER DLT SYSTEM, THEIR SPECIFIC ROLES AND EXPERIENCE

DLT system	Total
Aragon	2
Ardor	2
Bitcoin	1
Blockstack	1
Byteball	1
Corda	2
Counterparty	1
Dash	6
Ethereum	1
Factom	1
Golem	1
Hyperledger (Fabric)	4
IOTA	3
Monero	4
Namecoin	1
Siacoin	1
Stellar	1
Storj	1
Zcash	2
Total	**36**

Role in Project	Total
Project Lead	9
Core/Team Developer	7
Team Member	6
Advisor	1
Community Developer	5
Community Member	2
Other	6
Total	**36**

Experience	Total
$>$ 3 years	14
1-3 years	16
$<$ 1 year	6
Total	**36**



(a) Classification (N=36,31) (b) Taxonomy (N=35)

Fig. 3. Rating of the classification and expressiveness of taxonomy components as perceived by survey participants

chain underlying (66.7%). Five attributes are above 90%: address traceability (100%), origin (94.4%), actor permission (93.3%), conditional creation (93.3%) and unconditional creation (93.3%).

Figure 4 shows, that the highest disagreements are observed with on-chain underlying (30.0%), validator permission (19.4%) and off-chain underlying (13.3%). The highest uncertainty is found with on-chain and off-chain underlying (each 20.0%), consensus type (19.4%), read permission (13.3%) and burn property (13.3%).

Having a detailed look at the comments provided by the participants who disagreed with the classification of the on-chain underlying, one notices the following[11]: On-chain storage of hashes is not seen as storage by participants (22.2%). For some systems, contradicting comments of the participants for the on-chain value of the systems token are stated (11.1%). Some participants mixed up the on-chain underlying of the token with the overall services that the DLT system provides (22.2%), which not necessarily need to be accessed via the token. Some participants disagree because the classification does not consider on-chain underlyings which are expected to be implemented in the future (33.3%). Other respondents confused the option to use a token as a currency with its underlying (22.1%). Finally, some mixed up on-chain underlying with off-chain underlying (11.1%).

[11]In brackets are depicted the percentage for which this responds type accounts to the overall disagreements. Please note, that the percentages do not add up to 100% as a survey participant could state several reasons for disagreement

Some of those, who answered that they are uncertain, did not distinguish current implementation of on-chain underlyings and future implementations (50.0%), which are not considered by the classification. Other respondents mixed up the possibility to use a token as a currency with its underlying (25.0%). Some identified a misformatted question formulation (25.0%).

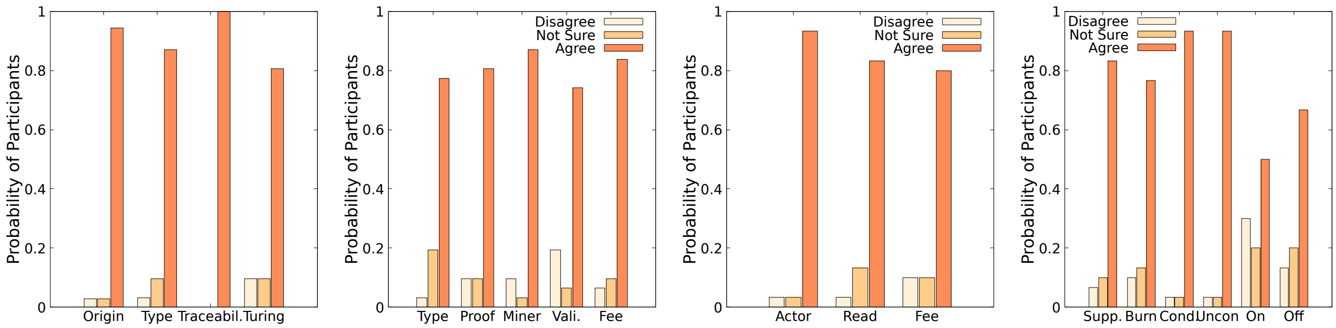
For the off-chain underlying a similar picture can be drawn. Here, the disagreement and uncertainty answers are combined: Participants considered past and future off-chain underlyings and disagreed with the classification (30.0%). Some understood off-chain underlying to be an exclusive right for the token (10.0%). Moreover, as in the on-chain case, some participants linked the possibility to use the token as a currency to its underlying (20.0%). Some participants mixed on-chain and off-chain value (10.0%), others did not understand the question (10.0%) or did not respond (20.0%).

To sum up, despite the fact that disagreements and uncertainties are significantly low, the main ones stated are outlined below:

1) Not distinguishing up on-chain and off-chain underlying
2) Not distinguishing the underlying from services which can be assessed in the DLT system
3) Mixing up the underlying with the possibility to use a token as a currency
4) Considering future or past features of the DLT systems
5) Rejecting on-chain storage of hashes as storage

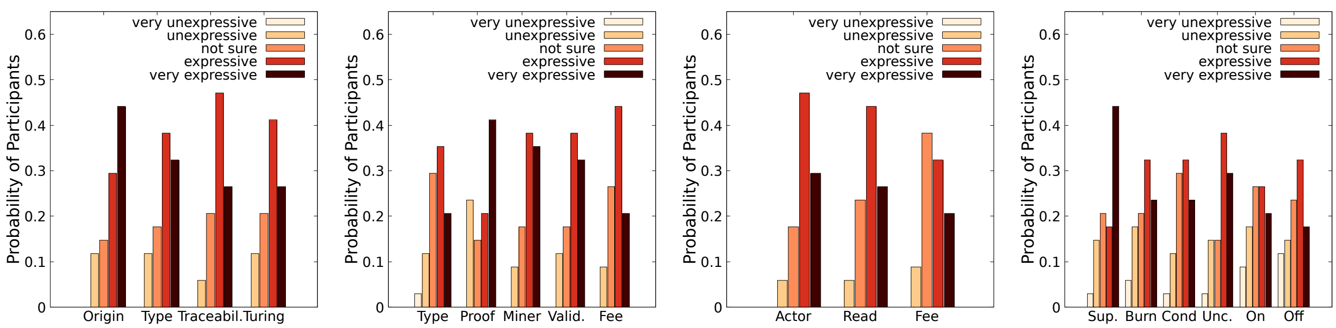
Furthermore, the feedback indicates that survey participants are in some instances inconsistent with the evaluation of the classification within a DLT system. For instance, as stated previously, some survey participants disagreed on the characteristic of a system's on-chain underlying. In order to investigate this further, the weighted consistency averages for each attribute are depicted in Figure 6. The values are calculated as follow: Assuming a linear scale for the responses: 0 - disagree, 1 - not sure, 2 - agree, the values are normalized to take values in the range $[0, 1]$. Then, for each DLT system from which more than one response is obtained as illustrated in Table VII, the consistency of responses is calculated for each system and attribute with the mean absolute error. Then, the average for each attribute is obtained by taking the weighted average of the DLT systems consistency values.

The overall consistency is on average 91.0%. The lowest consistency is measured for the on-chain and off-chain underlying, correlating with the higher disagreements observed



(a) Distributed Ledger (N=36,31) (b) Consensus (N=31) (c) Action (N=30) (d) Token (N=30)

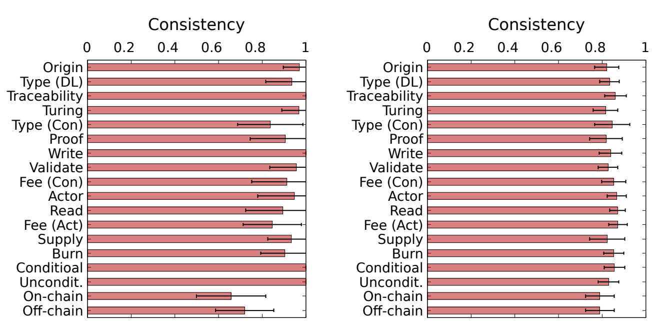
Fig. 4. Classification evaluation of the attributes, clustered componentwise



(a) Distributed Ledger (b) Consensus (c) Action (d) Token

Fig. 5. Expressiveness evaluation of the attributes, clustered componentwise (N=34)

earlier. The highest consistencies are noticed for address traceability, write permission, conditional creation and unconditional creation.



(a) Agreement on Classification (N=25,24,23) (b) Expressiveness of Taxonomy (N=23)

Fig. 6. Weighted average of consistency calculation per attribute, using DLT systems consistency values of which more than one response is obtained

C. Incorporating Blockchain Community Feedback

Motivated by the received feedback, three changes to the taxonomy are introduced.

First, in order to reduce the ambiguity when it comes to mixing up on-chain underlyings, off-chain underlyings and other services in the system and hence addressing point one and two of the previous summary, a more clear mapping of the token underlying to the components of the conceptual framework (Figure 1) is introduced. For that, the off-chain and on-chain underlyings are merged into one attribute and their characteristics are abstracted to take values in the component of the framework where the underlying resides on. For instance, in case of the Ethereum token: Instead of expressing, that the token gives access to the on-chain underlying *computation*, the token is now said to provide access to the *distributed ledger*, which in turn implies giving access to computation.

Second, in order to emphasize the possibility to store arbitrary data on distributed ledgers (e.g hashes), which, for instance, enables Bitcoin to function as an infrastructure system, the storage attribute has been added to the distributed ledger component. This addresses point number five.

Third, in order to address point number three, the transferability attribute has been added to the token component, which emphasizes the possibility to use the token as a currency. Because the classification captures the current state of DLT systems and not future possible extensions, point number four is not addressed.

D. Taxonomy

In this second part of the survey, the blockchain community is asked to evaluate the developed taxonomy. Nickerson et al. propose five criteria to assess the “usefulness” of a taxonomy [23]. Namely, a taxonomy is

- *concise*, if it uses a limited number of attributes and characteristics,
- *robust*, if it uses enough attributes and characteristics to clearly, *differentiate* the objects of interest
- *comprehensive*, if it can *classify* all known objects within the domain under considerations,
- *extensible*, if it allows for inclusion of additional dimensions and new characteristics within a dimension when new types of objects appear,
- *explanatory*, if it contains object attributes and characteristics that do not model every possible detail of the objects but, rather, provide useful explanations of the nature of the objects under study or help to understand future objects.

The literature review (Section II) reveals an ambiguity in how many attributes and characteristics should be included in a taxonomy of DLT systems. Moreover, the classification considers DLT systems discussed in academic literature, hence the taxonomy should enable such a classification. Considering these two points, the taxonomy is evaluated using the robustness and comprehensiveness criteria of Nickerson et al. [23]:

For that, this paper introduce the concept of expressiveness:

Definition 5. *A taxonomy is expressive when it is robust and comprehensive.*

The perceived expressiveness of the developed taxonomy can be determined by asking the survey participants for each component and attribute:

Question 1. *"How expressive is [component/attribute] to differentiate between and classify DLT systems".*

This question reveals the concept of expressiveness, comprehensiveness and robustness to the survey participants, with neither exposing them to the theory nor overloading them with a high number of questions.

Figure 3(b) depicts the expressiveness of the four components as perceived by the survey participants. The consensus component is seen as the most expressive (82.9%), followed by distributed ledger (80.0%), token (62.9%) and action (54.3%). The highest uncertainties are measured with the action (34.3%) and token (28.6%) components. This paper is the first to introduce an action and a token component, which focuses on the cryptoeconomic design of a DLT system. The lower rating of expressiveness of the token and action components and the significant higher uncertain ratings when compared to the consensus and distributed ledger component account for this. In particular, the consensus component is used by all terminologies found in literature (Section II) and thus must be familiar to survey participants. Moreover, the action component consists of the least number of attributes, which may decrease the perceived expressiveness. In particular, the reduced number of attributes seems to hinder the differentiation between DLT systems.

Twelve participants comment on the expressiveness of the components. They state that governance, funding of DLT systems and the development strategy of the source code should be included (16.7%). One participant mentions, that the action component is not expressive enough, because it lacks attributes which would express the unique features of the system (8.3%). Similar statements have been formulated for other components (25.0%). Another participant does not think that developing a taxonomy for blockchain systems is useful (8.3%). Finally, some participants made statements endorsing the construction of the taxonomy (42.7%).

Figure 5 depicts the experessiveness of the 18 attributes. The four most expressive attributes are actor permission (76.5%), DL origin (73.5%), address traceability (73.5%) and write permission (73.5%). Action fee (38.2%), conditional creation (29.4%) and consensus type (29.4%) raise the highest uncertainties. The most unexpressive attributes are on/off-chain underlyings (each 26.5%), burn property (23.5%) and consensus proof (23.5%). The lower values for the underlyings are supposedly due to the lower classification ratings. Despite the action component being the least expressive component, its attribute of actor permission is rated as the most expressive and also its other two attributes are among the top-9 most expressive ones. This strengthens the suggestion to extend the action component with further attributes.

Figure 6(b) depicts the consistency with which the participants evaluated the expressiveness of the taxonomy attributes. Despite normalizing a five point likert scale (0-very unexpressive, 1-expressive, 2-not sure, 3-expressive, 4-very expressive) to take values in zero to one, the calculation of the consistency remains the same as for the classification. The average consistency over all attributes is 83.7%, meaning that survey participants of the same DLT system rated the expressiveness of the taxonomy similar to each other. In particular, they diverge on average only 16.3% from each other, which resembles fewer than one choice difference on the constructed likert-scale. Moreover, one notices, that the 10% confidence intervals overlap for all weighted averages.

VII. Conclusion and Outlook

This paper distinguishes cryptoeconomic design from the distributed ledger and consensus of a DLT system. Based on this modeling separation, a novel conceptual architecture for DLT systems is introduced, which in turn allows the construction of an expressive taxonomy as defined in Section VI-D based on taxonomy theory and validated by feedback collected from blockchain community to harvest wisdom of the crowd. The significance of this approach lies in the fact that, unlike other compared approaches found in academic literature (Section II), all taxonomy components (distributed ledger, consensus, action, token) are derived from the architecture. This justifies and positions the taxonomy components and attributes as well as motivates their interrelationships. The taxonomy is then used to reason about yet undefined cryptoeconomic terminologies, such as permissionless systems or asset tokens using Boolean Algebra. The latter play an important role for the swiss financial market authority FINNMA to classify a token as a security [40].

The effectiveness and applicability of the taxonomy is then demonstrated by classifying systems found in academic literature. The fact that 29 of those DLT systems of different design approaches can be uniquely classified indicates a high robustness as motivated in earlier taxonomy theory [23] and discussed in Section VI-D.

The feedback of the blockchain community is studied and turned into concrete improvement actions applied to the final proposed taxonomy. In particular, the restructuring of the underlying attribute improves its conciseness. Moreover, the feedback further confirms the comprehensiveness and robustness of the taxonomy as shown in Figure 3(b) with a 70% expressiveness on average and the ones of the classification in Figure 3(a) with 83% agreement on average.

The results point to different directions for future research. First, given that the DLT systems are an area of active research in industry and academia, it is expected that the conceptual framework can be challenged by new systems, particularly by system designs diverging from the architectures that are considered typical at the time of writing this paper, for instance permissionless blockchain systems with PoW consensus. Particularly, one can further explore the token design space and conceptualize systems with more than one token, e.g. the Akasha systems uses several tokens [34]. Second, the evaluation suggests that the taxonomy can be further extended with further attributes for the action component, such as the type of actions, which can be performed in the system. Moreover, the consensus component can be extended with a network topology attribute or the underlying attribute can be restructured into an on-chain and off-chain underlying. Furthermore, a component modeling inter-token relationships or the governance of the systems can become a requirement. Especially the latter can be critical in deciding if a system has a decentralized organization (e.g. no trusted party). Nevertheless, it needs to be evaluated how far these extensions affect the expressiveness or conciseness of the taxonomy. The possibility of grouping a larger number of DLT systems with similar attribute characteristics, as demonstrated in Section V (e.g. permissionless systems), suggests to perform a cluster analysis on top of the classification accompanied by further large-scale community feedback.

Acknowledgment

This work is supported by the Swiss National Science Foundation (grant no. 170226) for the European FLAG ERA project 'FuturICT 2.0 - Large scale experiments and simulations for the second generation of FuturICT' (https://futurict2.eu/) and the European Communitys H2020 Program under the scheme 'ICT-10-2015 RIA', grant agreement #688364 'ASSET: Instant Gratification for Collective Awareness & Sustainable Consumerism' (http://www.asset-consumerism.eu).

In addition, the authors would like to thank Michael Noack, Qusai Jouda and Max Roessner for their support in the questionnaire development and the proof reading of the classification.

References

[1] A. Tapscott and D. Tapscott, "How blockchain is changing finance," *Harvard Business Review*, vol. 1, 2017.

[2] X. Xu, I. Weber, M. Staples, L. Zhu, J. Bosch, L. Bass, C. Pautasso, and P. Rimba, "A taxonomy of blockchain-based systems for architecture design," in *Software Architecture (ICSA), 2017 IEEE International Conference on*. IEEE, 2017, pp. 243–252.

[3] K. Korpela, J. Hallikas, and T. Dahlberg, "Digital supply chain transformation toward blockchain integration," in *proceedings of the 50th Hawaii international conference on system sciences*, 2017.

[4] A. Manohar and J. Briggs, "Identity management in the age of blockchain 3.0," 2018.

[5] J. Kang, R. Yu, X. Huang, S. Maharjan, Y. Zhang, and E. Hossain, "Enabling localized peer-to-peer electricity trading among plug-in hybrid electric vehicles using consortium blockchains," *IEEE Transactions on Industrial Informatics*, vol. 13, no. 6, pp. 3154–3164, 2017.

[6] N. Kshetri and J. Voas, "Blockchain-enabled e-voting," *IEEE Software*, vol. 35, no. 4, pp. 95–99, 2018.

[7] J. Bonneau, A. Miller, J. Clark, A. Narayanan, J. A. Kroll, and E. W. Felten, "Sok: Research perspectives and challenges for bitcoin and cryptocurrencies," in *2015 IEEE Symposium on Security and Privacy*, May 2015, pp. 104–121.

[8] F. Tschorsch and B. Scheuermann, "Bitcoin and beyond: A technical survey on decentralized digital currencies," *IEEE Communications Surveys & Tutorials*, vol. 18, no. 3, pp. 2084–2123, 2016.

[9] D. Babbitt and J. Dietz, "Crypto-economic design: A proposed agent-based modeling effort," in *English. Conference Talk. University of Notre Dame, Notre Dame, USA*, 2014.

[10] S. Davidson, P. De Filippi, and J. Potts, "Economics of blockchain," *SSRN Working Paper No 2744751, Available at SSRN: https://ssrn.com/abstract=2744751*, 2016.

[11] B. Notheisen, F. Hawlitschek, and C. Weinhardt, "Breaking down the blockchain hype–towards a blockchain market engineering approach," *In: Proceedings Americas Conference on Information Systems*, 2017.

[12] R. E. Samuel, "A layered architectural approach to understanding distributed cryptographic ledgers." *Issues in Information Systems*, vol. 17, no. 4, 2016.

[13] P. Tasca and C. Tessone, "Taxonomy of blockchain technologies. principles of identification and classification," *SSRN Working Paper No 2977811, Available at SSRN: https://ssrn.com/abstract=2977811*, 2017.

[14] K. Yeow, A. Gani, R. W. Ahmad, J. J. Rodrigues, and K. Ko, "Decentralized consensus for edge-centric internet of things: A review, taxonomy, and research issues," *IEEE Access*, vol. 6, pp. 1513–1524, 2018.

[15] X. Xu, C. Pautasso, L. Zhu, V. Gramoli, A. Ponomarev, A. B. Tran, and S. Chen, "The blockchain as a software connector," in *Software Architecture (WICSA), 2016 13th Working IEEE/IFIP Conference on*. IEEE, 2016, pp. 182–191.

[16] M. Comuzzi, E. Unurjargal, and C. Lim, "Towards a design space for blockchain-based system reengineering," in *International Conference on Advanced Information Systems Engineering*. Springer, 2018, pp. 138–143.

[17] H. Okada, S. Yamasaki, and V. Bracamonte, "Proposed classification of blockchains based on authority and incentive dimensions," in *Advanced Communication Technology (ICACT), 2017 19th International Conference on*. IEEE, 2017, pp. 593–597.

[18] J. De Kruijff and H. Weigand, "Towards a blockchain ontology," *Research report Tillburg University*, 2017.

[19] M. Morisse, "Cryptocurrencies and bitcoin: Charting the research landscape," *In: Proceedings Americas Conference on Information Systems*, 2015.

[20] V. Dhillon, D. Metcalf, and M. Hooper, "Decentralized organizations," in *Blockchain Enabled Applications*. Apress, Berkeley, CA, 2017, pp. 47–66.

[21] L. S. Sankar, M. Sindhu, and M. Sethumadhavan, "Survey of consensus protocols on blockchain applications," in *Advanced Computing and Communication Systems (ICACCS), 2017 4th International Conference on*. IEEE, 2017, pp. 1–5.

[22] D. Mingxiao, M. Xiaofeng, Z. Zhe, W. Xiangwei, and C. Qijun, "A review on consensus algorithm of blockchain," in *Systems, Man, and Cybernetics (SMC), 2017 IEEE International Conference on*. IEEE, 2017, pp. 2567–2572.

[23] R. C. Nickerson, U. Varshney, and J. Muntermann, “A method for taxonomy development and its application in information systems,” *European Journal of Information Systems*, vol. 22, no. 3, pp. 336–359, 2013.

[24] I. ISO, “Ieee: Iso/iec/ieee 42010: 2011-systems and software engineering–architecture description,” *Proceedings of Technical Report*, 2011.

[25] J. L. de la Rosa, V. Torres-Padrosa, A. el Fakdi, D. Gibovic, O. Hornyák, L. Maicher, and F. Miralles, “A survey of blockchain technologies for open innovation,” in *4rd Annual World Open Innovation Conf. WOIC*, 2017, pp. 14–15.

[26] K. P. Kalinin and N. G. Berloff, “Blockchain platform with proof-of-work based on analog hamiltonian optimisers.” [Online]. Available: http://arxiv.org/abs/1802.10091 (Accessed: 2018-03-08).

[27] Z. Kakushadze and R. P. Russo Jr, “Blockchain: Data malls, coin economies and keyless payments,” *SSRN Working Paper No 2744751, Available at SSRN: https://ssrn.com/abstract=2744751*, 2018.

[28] J. Peterson, J. Krug, M. Zoltu, A. K. Williams, and S. Alexander, “Augur: a decentralized oracle and prediction market platform,” 2018.

[29] J. Bonneau, A. Miller, J. Clark, A. Narayanan, J. A. Kroll, and E. W. Felten, “Sok: Research perspectives and challenges for bitcoin and cryptocurrencies,” in *Security and Privacy (SP), 2015 IEEE Symposium on*. IEEE, 2015, pp. 104–121.

[30] P. Moreno-Sanchez, T. Ruffing, and A. Kate, “Pathshuffle: Credit mixing and anonymous payments for ripple,” *Proceedings on Privacy Enhancing Technologies*, vol. 2017, no. 3, pp. 110–129, 2017.

[31] “The Anatomy of a Transaction.” [Online]. Available: https://domschiener.gitbooks.io/iota-guide/content/chapter1/transactions-and-bundles.html (Accessed: 2018-09-06).

[32] L. Lamport, R. Shostak, and M. Pease, “The byzantine generals problem,” *ACM Transactions on Programming Languages and Systems (TOPLAS)*, vol. 4, no. 3, pp. 382–401, 1982.

[33] “Ripple transacton cost.” [Online]. Available: https://developers.ripple.com/transaction-cost.html (Accessed: 2018-09-06).

[34] F. A. B. Thoughts and P. Updates, “New horizons.” [Online]. Available: http://blog.akasha.world/2017/11/14/new-horizons/ (Accessed: 2018-09-05).

[35] “Steemit whitepaper.” [Online]. Available: https://steem.io/steem-whitepaper.pdf (Accessed: 2018-09-06).

[36] “Xrp ledger overview.” [Online]. Available: https://developers.ripple.com/transaction-cost.html (Accessed: 2018-09-06).

[37] “Dash whitepaper.” [Online]. Available: https://github.com/dashpay/dash/wiki/Whitepaper (Accessed: 2018-09-06).

[38] “SiaHub.” [Online]. Available: https://siahub.readme.io/reference (Accessed: 2018-09-06).

[39] L. Wu, K. Meng, S. Xu, S. Li, M. Ding, and Y. Suo, “Democratic centralism: A hybrid blockchain architecture and its applications in energy internet,” in *2017 IEEE International Conference on Energy Internet (ICEI)*, pp. 176–181.

[40] E. F. FINMA, “FINMA publishes ICO guidelines.” [Online]. Available: https://www.finma.ch/en/news/2018/02/20180216-mm-ico-wegleitung/ (Accessed: 2018-07-27).

[41] “Aragon,” https://aragon.org/, (Accessed: 2018-04-01).

[42] “Ripple - one frictionless experience to send money globally,” https://ripple.com/, (Accessed: 2018-04-01).

[43] “Peercoin,” https://peercoin.net/, (Accessed: 2018-04-01).

[44] “Monero,” https://getmonero.org/, (Accessed: 2018-04-01).

[45] “Hyperledger Fabric.” [Online]. Available: https://www.hyperledger.org/projects/fabric (Accessed: 2018-09-06).

[46] “Dash,” https://www.dash.org/, (Accessed: 2018-04-01).

[47] “Augur - a decentralized oracle & prediction market protocol,” https://www.augur.net, (Accessed: 2018-04-01).

[48] “Dogecoin,” https://dogecoin.com/, (Accessed: 2018-04-01).

[49] “Zcash - All coins are created equal.” [Online]. Available: https://z.cash/ (Accessed: 2018-09-06).

[50] T. Ruffing, P. Moreno-Sanchez, and A. Kate, “P2p mixing and unlinkable bitcoin transactions.” in *Network and Distributed System Security Symposium (NDSS)*, 2017.

[51] “EOS,” https://eos.io/, (Accessed: 2018-04-01).

[52] “Byteball - a cryptocurrency platform ready for real world adoption,” https://byteball.org/, (Accessed: 2018-04-01).

[53] “Golem,” https://golem.network/, (Accessed: 2018-04-01).

[54] “Stellar - Develop the world’s new financial system.” [Online]. Available: https://www.stellar.org/ (Accessed: 2018-09-06).

[55] “Factom - Making the World’s Systems Honest.” [Online]. Available: https://www.factom.com/ (Accessed: 2018-09-06).

[56] “Namecoin.” [Online]. Available: https://namecoin.org/ (Accessed: 2018-09-06).

[57] “Omni Layer,” https://www.omnilayer.org/, (Accessed: 2018-04-01).

[58] “Decentralized Cloud Storage Storj.” [Online]. Available: https://storj.io/ (Accessed: 2018-09-06).

[59] “Sia.” [Online]. Available: https://sia.tech/ (Accessed: 2018-09-06).

[60] “SAFE Network - Secure Access For Everyone.” [Online]. Available: https://safenetwork.org/ (Accessed: 2018-09-06).

[61] “Blockstack.” [Online]. Available: https://blockstack.org/ (Accessed: 2018-09-06).

[62] “Filecoin.” [Online]. Available: https://filecoin.io/ (Accessed: 2018-09-06).

[63] “Ethereum Project.” [Online]. Available: https://www.ethereum.org/ (Accessed: 2018-09-06).

[64] “Corda — Home.” [Online]. Available: https://www.corda.net/ (Accessed: 2018-09-06).

[65] “Counterparty.” [Online]. Available: https://counterparty.io/ (Accessed: 2018-09-06).

[66] “Enigma We’re Making Decentralization Work.” [Online]. Available: https://enigma.co/ (Accessed: 2018-09-06).

[67] “The Next Generation of Distributed Ledger Technology.” [Online]. Available: https://www.iota.org/ (Accessed: 2018-09-06).

[68] “Litecoin — Money for the Internet Age.” [Online]. Available: https://litecoin.com/ (Accessed: 2018-09-06).

[69] “Block chain - Bitcoin Wiki.” [Online]. Available: https://en.bitcoin.it/wiki/Block_chain (Accessed: 2018-02-22.

[70] “Ardor.” [Online]. Available: https://www.ardorplatform.org/ (Accessed: 2018-09-06).

[71] H. Shafagh, L. Burkhalter, A. Hithnawi, and S. Duquennoy, “Towards blockchain-based auditable storage and sharing of IoT data,” in *Proceedings of the 2017 on Cloud Computing Security Workshop*. ACM, 2017, pp. 45–50.

[72] J. Sousa, A. Bessani, and M. Vukolic, “A byzantine fault-tolerant ordering service for the hyperledger fabric blockchain platform,” in *2018 48th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN)*. IEEE, 2018.

[73] V. Dhillon, D. Metcalf, and M. Hooper, “Recent developments in blockchain,” in *Blockchain Enabled Applications*. Apress, Berkeley, CA, 2017, pp. 151–181.

[74] T. Liu, Z. Tariq, J. Chen, and B. Raghavan, “The barriers to overthrowing internet feudalism,” in *Proceedings of the 16th ACM Workshop on Hot Topics in Networks*, ser. HotNets-XVI. ACM, 2017, pp. 72–79. [Online]. Available: http://doi.acm.org/10.1145/3152434.3152454

[75] P. M. Krafft, N. Della Penna, and A. S. Pentland, “An experimental study of cryptocurrency market dynamics,” in *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems*. ACM, 2018, p. 605.

[76] G. Zyskind, O. Nathan, and A. Pentland, “Enigma: Decentralized computation platform with guaranteed privacy,” *arXiv preprint arXiv:1506.03471*, 2015.