New kid on the block: a strategic archetypes approach to understanding the Blockchain

Clara Walsh
University College Cork
Ireland
clara.walsh@umail.ucc.ie

Philip O’Reilly
University College Cork
Ireland
philip.oreilly@ucc.ie

Rob Gleasure
University College Cork
Ireland
r.gleasure@ucc.ie

Joseph Feller
University College Cork
Ireland
jfeller@ucc.ie

Shanping Li
Zhejiang University
China
shan@zju.edu.cn

Jerry Cristoforo
State Street Corporation
jacristoforo@statestreet.com

Abstract

Emerging Blockchain technologies have received considerable attention in the financial services domain. This is due to the potential of those technologies to radically disrupt existing financial systems by introducing new types of assets and new ways of managing transactions. Yet many of these technologies are so new and seemingly complex that strategic decision-makers may not fully understand the alternative Blockchain technologies on offer, let alone the costs and benefits associated with specific instantiations. This paper reviews the Blockchain literature and identifies eight key system design characteristics. From this, four Blockchain archetypes emerge, each of which is presented using a recognizable existing system to allow tangible discussion of similarities and differences across archetypes. The identification of these archetypes provides an important foundation for future research, enabling in-depth research to be conducted that will outline the costs, benefits, risks, and issues associated with each archetype.

Keywords: Blockchain, Strategic Archetypes, Cryptocurrency, Bitcoin
Introduction

In the past eighteen months, there has been a significant increase in interest among financial services companies regarding Blockchain technology. Big financial services players are backing and sponsoring a wide range of Blockchain initiatives, both company specific and consortia based (Van Steenis et al. 2016). For example, R3 has established a consortium to collaborate on advancing Blockchain research for potential adoption within financial services, a consortia that includes over 40 of the world's leading banks and leading technology companies, such as Microsoft. On New Year's Eve 2015, Nasdaq enabled the first-ever private securities issuance on their new Blockchain technology platform: Nasdaq Linq. Nasdaq purport that Blockchain holds the potential for 99% reduced settlement time and risk exposure in capital markets (Nasdaq 2015). The number of such projects is ever increasing and other institutions researching Blockchain technologies include State Street, BNP Paribas and Goldman Sachs (BitFury Group and Garzik 2015).

While it is purported that Blockchain has the potential to transform aspects of financial services, a closer examination of Blockchain reveals that there are numerous models of Blockchain implementation (He et al. 2016) with no ‘one size fits all’ instantiation. Yet, the design characteristics of Blockchain models remain under-investigated. Furthermore, while there is significant hype and focus on the technological characteristics of Blockchain, actual adoption of Blockchain technologies in the financial services domain remains low (Peters and Panayi 2015; Fico 2016) and significant obstacles must be overcome to ensure that the changes which Blockchain brings about will be accepted by users (Malik 2016; Tripathi 2016). Therefore, a key question to be addressed if Blockchain is to achieve the proposed commercial benefits is: what are the different types of Blockchain technologies available and what are their associated strategic strengths and weaknesses?

This research-in-progress study seeks to begin addressing this question. First, we discuss a strategic archetypes approach to Blockchain systems. Next, we extend existing Blockchain research by presenting four Blockchain archetypes based on a state of the art literature review, conducted by utilising the hermeneutic approach purported by Boell and Ceez-Kecmanovic (2014) for undertaking literature, with the focus being on developing understanding, continuous engagement and iterative development. This review identifies eight key features of Blockchain technologies, from which four system archetypes emerge. These archetypes capture frequently occurring, named groupings with similar configurations across multiple attributes (c.f. Soh and Markus 2002), the identification of which will enable the strengths and weaknesses of different Blockchain models to be empirically investigated.

Strategic Archetypes and Blockchain

The importance of strategic alignment for new IT is well-established in IS literature (Miller 1988; Henderson and Venkatraman 1999; Powell and Dent-Micalef 1997; Reich and Benbasat 2000; Kearns and Sabherwal 2006). Yet many new technologies can be characterized according to so many different attributes that it is difficult for non-specialists to understand the different capabilities on offer, let alone compare and contrast comparable alternatives. Soh and Markus (2002) argued that the use of technological archetypes for complex systems is a useful means of assessing their potential alignment in a holistic manner, rather than trying to manage alignment at a bivariate-level (comparing existing systems with new technologies at the level of specific attributes). Indeed, the use of such archetypes and recognizable narratives is a common method of sense-making for individuals faced with learning about multi-faceted new phenomena (Trice and Beyer 1984; Orbuch 1997).

The concept of an archetype implies some form of classification (Soh and Markus 2002; Greenwood and Hinnings 1993). Such classification requires coherence between elements if typologizing is to be performed sensibly, as well as the development of classifications based upon thematic differences and similarities in overall patterns (Greenwood and Hinnings 1993; Miller 1996). This demands that an effective archetype provides a configured structure, expressing underlying values that make sense of contained relationships between attributes (Deephouse 1999; Greenwood and Hinnings 1993).

From a Blockchain perspective, this suggests two steps to identify useful archetypes (i) identify the key attributes that characterize the technology (ii) find some thematic structure allowing these attributes to be organized in a way that is both theoretically sensible and empirically grounded.
Key Attributes of Blockchain Technologies

Blockchain is an important emerging phenomenon with the potential for significant economic and business effects (O’Reilly 2016). Different Blockchain systems are designed to reflect different requirements, notably around speed, efficiency, security and transparency (He et al. 2016). From a technological perspective, Blockchain can be viewed as a peer-to-peer infrastructure where nodes representing individuals in the network coordinate to process transactions (O’Reilly 2016). At the heart of this is a ‘distributed ledger’, a continuously growing history of records stored in a chain that are hardened against tampering and revision by the use of cryptographic algorithms (Glaser et al. 2014). The Blockchain is immutable, meaning transactions cannot be changed/deleted once added to the Blockchain. This allows Blockchains to act as a reputable source of unchangeable, verified and valid information (Peters and Panayi 2015).

A review of the literature reveals eight discriminatory characteristics of Blockchain systems (see Table 1): (1) level of permission restrictions (2) level of restricted public access to data (3) level of investment-weighting for transaction consensus (4) level of chain modularity (5) level of scalability (6) level of interoperability (7) level of centralized regulation (8) level of anonymity.

<table>
<thead>
<tr>
<th>Characteristic</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Level of permission restrictions</td>
<td>The transaction processor parties who submit data and are eligible to create blocks of data. Two models exist (1) Permissioned (transaction processing performed by predefined users) and (2) Permissionless (no restrictions on identities of processors).</td>
</tr>
<tr>
<td>Level of restricted public access to data</td>
<td>The organization that can view Blockchain data. Two model exists (1) Public, where there are no restrictions on reading Blockchain data and (2) Private, where direct access to Blockchain data is limited to predefined users.</td>
</tr>
<tr>
<td>Level of investment-weighting for transaction consensus</td>
<td>A means to determine consensus for new transactions and the current state of the system. Ensuring that transactions will only be added to the Blockchain when valid and never recorded more than once. Two models dominate (1) Proof-of-Work: Solving a computational difficult problem to ensure validity of new transactions and (2) Proof-of-Stake: The ability to create a new block depends on user’s ownership to the system.</td>
</tr>
<tr>
<td>Level of chain modularity</td>
<td>Asset characteristics (single &amp; multiple) issued by users of the Blockchain. Assets can either remain solely on the Blockchain (on chain) or can be held externally to the Blockchain in external distributed hash tables (off chain).</td>
</tr>
<tr>
<td>Level of scalability</td>
<td>The number of transactions processed per second impacted by the latency between transactions and each block size.</td>
</tr>
<tr>
<td>Level of interoperability</td>
<td>Ability of a Blockchain system to communicate/exchange information with other Blockchains. Overlay protocols and pegged sidechains facilitate interoperability.</td>
</tr>
<tr>
<td>Level of centralized regulation</td>
<td>The non-technology based mechanism by which belief and reliability is created in the Blockchain ecosystem. These may be created either via (1) a trust node (2) decentralized disintermediation and (3) a Blockchain provider.</td>
</tr>
<tr>
<td>Level of anonymity</td>
<td>Whether the identity of a user on the Blockchain is openly transparent.</td>
</tr>
</tbody>
</table>

Table 1: Blockchain Characteristics

Viewed thematically, these eight characteristics divide into two categories describing different approaches to network design. The first category describes the extent to which a network is evenly distributed or nuclear in terms of ownership and administration, i.e. Network Decentralization. This includes the level of permission restrictions, the level of restricted public access to data, the level of investment-weighting...
for transaction consensus, and the level of centralized regulation. Greater levels of each of these variables will result in networks that are more centralized around specific nodes, whereas lower levels will result in administratively ‘flatter’ networks.

The second category describes the extent to which the boundaries for a network are open to new individuals, organizations, and technologies, i.e. Network Extensibility. This includes the level of scalability, the level of interoperability, the level of anonymity, and the level of chain modularity. Greater levels of each of these factors will result in more socially and technologically expansive networks.

**Emerging archetypes**

Four possible approaches to Blockchain design emerge based upon the two high-level categories, i.e. Decentralized/Extensible, Decentralized/Inextensible, Centralized/Extensible, and Centralized/Inextensible (see Figure 1).

Rather than discussing archetypes for each quadrant as abstract entities, four popular systems are selected as empirical exemplars, i.e. Bitcoin, Counterparty, Ripple, and R3. These four systems are not a perfect fit with the four quadrants, however they provide a tangible, empirically grounded, and relatable basis for discussion with strategic decision-makers.
Table 2: Blockchain Archetypes

<table>
<thead>
<tr>
<th></th>
<th>Bitcoin</th>
<th>Counterparty</th>
<th>Ripple</th>
<th>R3</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Level of permission restrictions</strong></td>
<td>Low</td>
<td>High</td>
<td>Medium</td>
<td>High</td>
</tr>
<tr>
<td><strong>Level of restricted public access to data</strong></td>
<td>High</td>
<td>High</td>
<td>Low</td>
<td>Low</td>
</tr>
<tr>
<td><strong>Level of investment-weighting for transaction consensus</strong></td>
<td>High (Proof-of-Work)</td>
<td>High (Proof-of-Work)</td>
<td>Low (Weighted Votes)</td>
<td>Low (Only parties involved in agreements)</td>
</tr>
<tr>
<td><strong>Level of chain modularity</strong></td>
<td>Low (On-chain, Single Asset)</td>
<td>Medium (Overlay Protocol, Digital Assets)</td>
<td>High (On-chain and Off-chain)</td>
<td>High (On-chain and Off-chain, Multiple Assets)</td>
</tr>
<tr>
<td><strong>Level of scalability</strong></td>
<td>Low (1MB Blocksize, Latency: 10 minutes, 7 transactions per second)</td>
<td>Low</td>
<td>High (Low latency, quick transaction transfers 3-6 seconds)</td>
<td>High (Only parties involved with agreements receive information)</td>
</tr>
<tr>
<td><strong>Level of interoperability</strong></td>
<td>Low (Overlay Protocols, Two-way Pegged Sidechains)</td>
<td>Medium</td>
<td>High (Standards, Integration with existing systems and different networks)</td>
<td>High</td>
</tr>
<tr>
<td><strong>Level of centralized regulation</strong></td>
<td>Low</td>
<td>Low</td>
<td>Low</td>
<td>High</td>
</tr>
<tr>
<td><strong>Level of anonymity</strong></td>
<td>High</td>
<td>Low</td>
<td>Medium</td>
<td>Low</td>
</tr>
</tbody>
</table>

Archetype 1: Bitcoin (Decentralized/Extensible)

The Bitcoin archetype is characterized by the fact that it is entirely transparent, decentralized and any party who has a copy of the Blockchain can begin broadcasting new transactions to the Blockchain without requiring prior authorization to do so (BitFury Group and Garzik 2015b; Tapscott and Tapscott 2016 p.67; Glaser et al. 2014).

In the Bitcoin archetype, a proof-of-work protocol is implemented to verify and validate transactions, build trust and secure the network from malicious attacks (Peters and Panayi 2015; Tapscott and Tapscott 2016 p.31, 259) as the users’ identity on the network aren’t known and are either pseudonymous or anonymous (Swanson 2015). Proof-of-work is a puzzle, which is complex to solve but effortless to verify, other users on the network are aware that a lot of resources (i.e. electricity and computing power) were exhausted when attempting to solve the mathematical puzzle and in turn trust the newly created block (BitFury Group 2015b; Tapscott and Tapscott 2016 p.31).

As mentioned, trust in the Bitcoin archetype is the result of the proof-of-work consensus protocol and computational difficult problems, which protect the system from malicious attacks (BitFury Group and
Garzik 2015b). Users don’t need to trust the users on the network, just the network itself (Dapp and Karollus 2015; Swan 2015 p.2).

Bitcoin is a single asset Blockchain used as a medium of exchange to transfer cryptographic tokens. The assets of the Bitcoin archetype are on-chain assets i.e. assets that are held on the Blockchain. Off-chain assets allow transactions to be conducted off the Blockchain, off-chain assets aren’t supported by the Bitcoin archetype because every node needs to have a copy of the Blockchain (Swanson 2015).

As the Bitcoin archetype is a decentralized network independent of a centralized entity all transactions are publicly available to all users resulting in a process, which is not influenced by a central institution (Glaser et al. 2014). A disadvantage to a lack of central control is that there is no regulatory body/watchdog overseeing the transactions of the network (Brezo and Bringas 2012). As mentioned above, users of Bitcoin transactions can be anonymous, however it might be possible to de-anonymize user’s identities by mapping Bitcoin user’s addresses to third party entities including currency exchanges and online wallets (Reid and Harrigan 2011).

This model is not without its challenges. The Bitcoin scripting language is limited, as it lacks a built in turing-complete scripting language, which enables the creation of smart contracts (BitFury Group 2015; Antonopoulos 2014 p.128). A non-turing-complete scripting language has limited complexity, one which doesn’t support complex loops (Antonopoulos 2014 p.128). Smart contracts are snippets of computational code carrying out ‘if-then’ functions, which are executed across the Blockchain nodes (Peters and Panayi 2015). Indeed, the Bitcoin scripting language is purposely not turing-complete so as not to introduce vulnerability to the network. (BitFury Group and Garzik, 2015; Antonopoulos 2014 p.128).

Interoperability with other Blockchains is not a feature of this archetype. However, the Bitcoin archetype can be extended by the use of protocols such as Colored Coin, which if implemented on top of the Bitcoin infrastructure allows different digital assets to be transferred on the Blockchain infrastructure (Rosenfeld 2012; Swanson 2015b). Bitcoin can also be extended to other Blockchains by the use of a sidechain (BitFury Group 2016). Sidechains allow bitcoins and other digital assets to be transferred between Blockchains by using a ‘two-way peg’, this is transferring assets off one blockchain to another and back to the original blockchain. (Back et al. 2014; Tapscott and Tapscott 2016 p.60).

The Bitcoin model is characterized by significant latency, as it can take up to 10 minutes for a new block to be generated (Croman et al. 2016; Tapscott and Tapscott 2016 p.32). A significant weakness of the Bitcoin archetype is scalability, each node on the network holds a copy of the Blockchain to verify transactions (Peters and Panayi 2015; Croman et al. 2016). As the amount of transactions increase, verifying transactions requires greater computational power and storage, resulting in some nodes not being able to scale to complete the proof-of-work. This may lead to: (1) a decrease in the number of users able to perform verification and (2) the network becoming more centralized (Peters and Panayi 2015; Croman et al. 2016). In this instance Bitcoin moves away from the Decentralized/Extensible archetype as the network should always remain decentralized.

Archetype 2: Counterparty (Decentralized/Inextensible)

Counterparty is an overlay asset protocol, which can be implemented on top of an existing Blockchain to apply additional functionality (BitFury Group 2016; Swan 2015 p.2; Antonopoulos 2014 p.220). Bitcoin lacks the native support for digital assets and smart contracts, however this functionality can be achieved with the help of an overlay protocol. Counterparty extends the Bitcoin protocol and creates auxiliary benefits such as transferring digital assets and the ability to run smart contracts on the Bitcoin Blockchain (Counterparty.io 2014; BitFury Group 2016).

Overlay protocols rely on the existing Blockchain infrastructure and the ability to store small amounts of data on the Blockchain (BitFury Group 2016). Bitcoin nodes are unaware of Counterparty’s existence and are completely oblivious to their assets (Counterparty.io 2014). The major benefit of Counterparty is the ability to create smart contracts (BitFury Group 2015). Counterparty allows users to implement smart contracts on the Bitcoin blockchain by writing turing-complete smart contracts, a notable difference from the Bitcoin archetype (Counterparty.io 2014).
This archetype further differs from the Bitcoin archetype, as it is a permissioned Blockchain. Before being able to add a new transaction or begin taking part in verifying the consensus protocol, users need to be authorized (BitFury Group and Garzik 2015). Individuals who want to run Counterparty software need to create a federated node. A federated node will run a full or partial copy of Counterparty software alongside the Bitcoin node (Counterparty.io 2016), those opting to create a federated node will be part of a small controlled group of users (Tapscott and Tapscott 2016 p.262). The advantage of this is that all users’ identity on the federated node is known so there is no anonymity. Thus, the possibilities of Sybil attacks are reduced in a public permissioned Blockchain, which is when a node can take the form of multiple identities/roles in an attempt to gain influence over the system (BitFury Group 2016; Tapscott and Tapscott 2016 p.36).

As the Bitcoin Blockchain implements proof-of-work to achieve consensus, Counterparty inherits this mechanism. Any transactions related to Counterparty are parsed from the Bitcoin Blockchain to a small local database. Counterparty requires a certain number of Bitcoin nodes to have a full copy of all transactions on the Blockchain (Counterparty.io 2015). Asset overlay protocols on the Bitcoin network such as Counterparty are not as scalable as Blockchains that support user-defined assets (BitFury Group 2016).

There are multiple projects using Counterparty software and tokens currently being developed, one company in particular, MandelDuck, is creating different apps which support Counterparty digital tokens (Campbell 2016). MandelDucks mission is developing games which facilitate interoperable apps where digital tokens can be transferred between apps by the use of a Blockchain (Mandelduck 2016). Another project working with Counterparty software is Storj.io, with the aim to create an instant micropayments channel. All Counterparty transactions are currently settled on the Bitcoin Blockchain, taking 10 minutes, this limits the scalability of Counterparty. The creation of a micropayments channel would potentially enable instant Counterparty transactions with the settlement happening on the Bitcoin blockchain at a later stage, which isn’t possible in Counterparty current implementation on the Bitcoin blockchain (Southurst 2016).

Archetype 3: Ripple (Centralized/Extensible)

The Ripple archetype is a private permissionless Blockchain. The goal of the Ripple archetype is to ‘make existing currencies more efficient’ (Swanson 2015) by providing global financial settlement systems, which allows banks to deal directly with each other, removing intermediaries (Piscini et al. 2016). In the Ripple archetype, users can access the blockchain when they have been authorized, only then do they have the right to use and read the Blockchain. Once you have been predefined to view the Blockchain, everyone can begin processing transactions and partaking in consensus validation (BitFury Group 2016; Rizzo 2016).

Ripple differs from a private permissionless blockchain because anyone is able to participate on the network. Ripple’s consensus protocol creates a set of rules, which allows user to participate in validating consensus with no permission required. To allow the network to grow and scale, Ripple can extend and revoke trust to participants to decide who can participate in the consensus validation (Kelleher 2015). The consensus protocol implemented by Ripple is different to other archetypes above, one involving no miners and no anonymous nodes to validate transactions (Tapscott and Tapscott 2016 p.67; Kelleher 2015). Ripple implements a collectively-trusted subnetwork within the larger network, meaning each node taking part in verifying if the transactions are valid come from a trusted set of nodes. The result is a low-latency consensus algorithm (Schwartz, Youngs and Britto 2014). Ripple transactions transfers take between 3 to 6 seconds and have fees which are transparent enabling real time settlement (Swanson 2015; Tapscott and Tapscott 2016 p.257). Ripple consensus protocol removes the need for anonymous miners who use a great deal of electricity implementing a proof-of-work protocol. This results in costs being kept down as transactions are validated by select group of members (Tapscott and Tapscott, 2016 p.67).

As the Ripple archetype is private, either on-chain or off-chain assets can be used. Off-chain assets allow transactions to be conducted off the Blockchain, allowing for a higher throughput of transactions (Poon and Dryja, 2016; Swanson 2015).
Ripple are working with other technological and financial services organization’s to develop technical standards for payments to facilitate a global real time Blockchain based payments system. The aforementioned standards would allow a means for different blockchain ledgers, for example Bitcoin and Ripple to interact and allow funds to move between Blockchains. This is a huge step towards global interoperability of systems (Ginder-Vogel 2016; Rizzo 2015).

Ripple is currently being used in a remittance proof-of-concept at the Royal Bank of Canada (RBC). The RBC performs large numbers of cross-border transactions every day, which involves multiple intermediaries, fees and can be a timely process. RBC looked to Ripple to try to increase efficiencies and lower costs, by connecting banks directly to each other and cut out the middleman. Ripple and RBC are working together on this remittance proof-of-concept to garner a better understanding about Blockchain scalability, security and performance (Piscini et al. 2016).

**Archetype 4: R3 (Centralized/Inextensible)**

The R3 archetype has many similarities with the Ripple archetype. A notable difference is once a party has been authorized to view the data in the R3 model, they also need to be authorized to broadcast transactions, which is not always the case in the Ripple archetype (BitFury Group 2016; Brown 2016). As R3 is a private permissioned decentralized model characterized as having high levels of trust, not all nodes have a copy of the Blockchain data (Peters and Panayi 2015). In relation to restrictions, R3 is different from the other archetypes as R3 doesn’t share entire information with everyone, only those parties concerned with a transaction can see the information (Brown 2016).

R3 Corda has been designed to support regulatory and supervisory nodes, which have capabilities to monitor the system, thereby increasing trust and reducing risk. R3 objectives are to build interoperable Blockchains facilitating greater monitoring of financial transactions by regulators and based upon agreed industry standards (Brown 2016). R3 are playing a critical role in the future of blockchain by creating standards to increase adoption of blockchain technology (Tapscott and Tapscott 2016 p.69).

The consensus protocol implemented by the R3 archetype is not at the system level but between the parties involved in individual deals. Transactions are validated by parties related to the transactions instead of a wide spectrum of users, unlike the other archetypes (Brown 2016).

As R3 Corda will have a smaller number of participants involved in the consensus mechanism, it will be much quicker to verify transactions than the permissionless archetypes mentioned earlier (BitFury Group 2016; Swanson 2015; Peters and Panayi 2015). A disadvantage to the R3 archetype is that by putting trust into a certain amount of participants, R3 limits the core aspect of Blockchain technology – trustlessness (BitFury Group and Garzik 2015).

In April 2016, UK Barclays Bank was the first to trial a smart contract prototype on R3 Corda. The prototype translated legal contracts into executable smart contract code by the use of a template. Once the contracts had been reviewed and approved by all parties, the smart contracts would then be stored on R3 Corda. Although all parties involved would be operating their own node, each party would be able to access the same smart contract-document on Corda and monitor any amendments to the original smart contract. (Rizzo 2016b).

**Proposed Method and Contribution**

This study aims to identify the strategic costs and benefits associated with each Blockchain archetype. To do this, an exploratory mixed-method approach is adopted (Creswell et al. 2007). This involves a sequential qualitative-dominant study design (Johnson et al. 2007; Venkatesh et al. 2013), whereby the qualitative component will be used to develop theory, while the quantitative component will test it.

Qualitative data gathering and analysis will take place within a case-study design (Benbasat et al. 1987; Darke et al. 1998). Case studies are one of the most commonly used research methods in the IS field (Benbasat et al. 1987; Darke et al. 1998), particularly when the aim is to obtain an in-depth understanding of some emerging phenomenon and its context (Cavaye 1996). Case studies enable researchers to investigate such phenomena without pre-defined limitations of control or manipulation of variables (Yin 1994; Cavaye 1996; Darke et al. 1998), thus are ideal when research is exploratory in nature (Marshall and
Rossman 1989; Galliers 1992). The primary source of data will be a series of semi-structured interviews conducted with financial services professionals. These professionals will be identified using criterion sampling, a specific type of purposeful sampling whereby the subjects for this study will have to meet predetermined criterion of importance stipulated by the researchers (Patton 2002), most notably in this instance this will require that participants are actively involved in research and development around Blockchain technologies.

Once a model has been developed from the qualitative component, a psychometric survey will be designed that uses reflective and/or formative measures for each construct to enable structural equation modelling of latent variables and hypothesized relationships (c.f. Gefen et al. 2000). This survey will be distributed to financial services professionals across a range of domains, further testing the legitimacy, explanatory power, and statistical generalizability of the proposed theory (Marshall and Rossman 1989; Yin 1994, Venkatesh et al. 2013).

This paper makes a number of contributions to the emerging Blockchain literature, which is at a very early stage of maturity. First, by analyzing extant literature and Blockchain instances, key Blockchain attributes are revealed. Understanding these different attributes allows for in-depth scholarly consideration at a feature-level, as well as encouraging scholars on the fringes of this subject matter to engage it in more detail.

Second, four Blockchain strategic archetypes emerged based on theoretical comparison of those attributes. This provides a simple theoretical baseline for Blockchain research, allowing findings from elaborate, domain or technology-specific instances to be reflected back to the broader set of technologies. Those archetypes also provide a means for less-granular consideration of systems, allowing less-technical researchers to engage with the technologies at a usage-level.

Third, this paper serves as a basis to enable further empirical investigation of the perceived costs and benefits associated with each archetype. Understanding those costs and benefits will allow strategic information systems researchers to begin a more lucid engagement with Blockchain technologies, as this model can be refined and extended as an increasing number of contexts are observed.

Furthermore, empirical investigation is also likely to uncover a number of operational issues associated with different archetypes, e.g. issues of governance, political aspirations, control, risk and resistance to change from those continuing to use traditional systems. This will further link this nascent area of research to other, more mature streams of theorizing.

Fourth, from a commercial perspective these strategic archetypes have significant potential in helping managerial decision-makers understand how specific Blockchain technologies might align with different goals and initiatives. This should create better dialogue between system designers and users, further guiding future development in a way that maximizes their disruptive commercial potential.

Acknowledgements

This research has been funded by State Street as part of the State Street EMEA Technology Centre located in University College Cork, Ireland.

References


Deephouse, D. 1999. "To be different, or to be the same? It’s a question (and theory) of strategic balance", *Strategic Management Journal*. (20:2), pp. 147-166.


