THE BITCOIN ECOSYSTEM: DISRUPTION BEYOND FINANCIAL SERVICES?

Research

Wörner, Dominic, ETH Zurich, Switzerland, dwoerner@ethz.ch

Von Bomhard, Thomas, University of St. Gallen, Switzerland, thomas.vonbomhard@unisg.ch

Schreier, Yan-Peter, University of St. Gallen, Switzerland

Bilgeri, Dominik, ETH Zurich, Switzerland

Abstract

The Bitcoin ecosystem has grown tremendously in recent years. While the main sectors of growth and venture capital funding have been infrastructure for the Bitcoin ecosystem itself as well as financial services, there is also a more recent evolution in sectors beyond financial services. We classify the venture-capital backed start up ecosystem accordingly and present its evolution over time. Thereby, we identify interesting sectors, i.e. digital assets, marketplaces, and notary services. Each sector is further subdivided, and six representative venture-backed start-up companies are presented in comprehensive case studies. We extract the core innovations and Bitcoin features on which these are based. Finally, we critically discuss their disruptive potential.

Keywords: Bitcoin, blockchain, start-up, radical innovation, disruptive innovation, case study, business model

1 Introduction

Incepting from a white paper (Nakamoto, 2008) published under the pseudonym Satoshi Nakamoto on a cypherpunk mailing list in late 2008 the first peer-to-peer electronic cash system – bitcoin – has developed into a global network of thousands of computers (with more than 5000 full nodes), a cryptocurrency with a market capitalization of more than $5B (Nov. 2015), and a vivid ecosystem of open source projects, start-up companies, as well as industry endeavours. According to recent data, almost $1B of Venture Capital has been invested in the bitcoin ecosystem since 2011 (CoinDesk, 2015).

Bitcoin is a particular implementation of a novel information technology, called blockchain, combining cryptography, peer-to-peer computing, and economic incentives to enable systems with networked trust. Instead of trusting a single custodian, system-wide consensus is reached by an ever-growing proof of computational work. Arguably, this technology has the potential for disintermediation and disruption (Baiyere et al., 2015), which is not limited to the financial service industry.

As shown by the literature review of Morisse (2015), the recent phenomena of cryptocurrencies has not yet reached mainstream IS research. Although there are several interesting links to IS research domains. For example, the social context of bitcoin as a currency has already been investigated by IS scholars: Glaser et al. (2014) and Hur et al. (2015) analysed the participation and intentions of bitcoin users. Ingram et al. (2015) explored the resilience of the bitcoin entrepreneurs facing the early crashes of the bitcoin currency like the bankruptcy of Mt. Gox (Dougherty and Huang, 2014).

However, as Giaglis and Kypriotaki (2014) have highlighted: an interesting area for IS scholars could be "to assist the transition from the first era of applications […] (i.e. bitcoin as currency) to more disruptive uses of the bitcoin protocol as an enabler of decentralized trusted peer-to-peer transaction ledger systems and applications." (p. 3) We've followed the development of the bitcoin ecosystem closely over the last years and acknowledge that practitioners are far ahead of IS scholars. A first technical taxonomy for decentralized consensus systems has been developed (Glaser et al., 2015). Moreover, digital business models of Bitcoin start-ups that depend mainly on the currency aspect of Bitcoin have been inspected in form of case studies (Kazan et al., 2015). We aim to advance the discussion beyond the cryptocurrency aspect and the financial service industry. Therefore our contribution is twofold. (1) We categorize the venture-backed Bitcoin start-up ecosystem along two dimensions, i.e. the potential for disruption and the particular sector, and present the evolution of the ecosystem since its inception. (2) Based on the categories, we investigate six companies in case studies with the aim to extract the core innovations and the features of Bitcoin that fuel those innovations, and critically discuss their potential for disruption.

The structure of the paper is as follows. In Section 2 we give a slightly technical introduction to Bitcoin as an implementation of a novel information technology. The focus thereby is on explaining the features that are utilized by the representative cases. In Section 3 we present the methodology by which we collected data, how we selected the cases, and how we analysed them. Section 4 is dedicated to the introduction and categorization of the Bitcoin start-up ecosystem, and we discuss its evolution over time. Thereafter, we present the case studies in Section 5, followed by key findings in Section 6. We conclude with a critical discussion of the disruptive potential and avenues for future research.

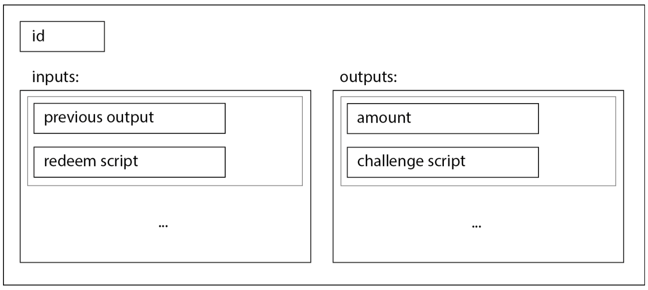

Figure 1. Simplified structure of a Bitcoin transaction.

2 Foundations

2.1 Bitcoin Primer

Bitcoin was introduced as a peer-to-peer electronic cash system (Nakamoto, 2008) that enables the pseudonymous transfer of value between untrusted parties over the Internet. Former efforts in digital currencies have relied on a central authority to prevent double spending. While digital coins can be authenticated by means of digital signatures there remains the problem of double spending. If, for example, Alice sends her coins simultaneously to Bob and Charlie, who owns them? A central trusted timestamp server, which unambiguously decides which transaction was first, solves this problem, but endeavours in this area have failed consistently in the past (McGullagh, 2001). Bitcoin provides a novel solution to the double spending problem: the blockchain and Nakamoto consensus. The Nakamoto consensus protocol is a practical solution to the Byzantine General's problem (Lamport et al., 1982) that does not require any trust in, or identities of, participants. This allows implementing a distributed timestamp server on a peer-to-peer basis. Special nodes in the network, called miners, vote on which transactions get included at a given point in time. In order to prevent Sybil attacks (Douceur, 2002), i.e. the creation of a large number of fake identities to bias the voting process, voting is facilitated according to contributed computing power in a process known as Proof-of-Work (Back, 2002). More comprehensible, the leader who is allowed to add transactions is determined by a kind of lottery with chances based on computing power. Since transactions get assembled into blocks and each block references its predecessor the emerging authenticated data structure is called a blockchain. The most important rule of the Nakamoto consensus protocol states that the valid chain is the longest chain, according to computational work. In this sense, the blockchain provides an immutable, append-only public database, which is secured by the computational power provided by miners. Miners are incentivized to provide their resources because the miner who solves the computational puzzle is allowed to claim newly minted bitcoins as well as the transaction fees included in the transactions of the particular block.

Surprisingly, there are no actual coins in the Bitcoin system, but only transactions. Each transaction consists of inputs and outputs, and each input has to reference an output of a previous transaction (see Figure 1 for illustration). There is only one exception: a coinbase transaction that is added by the miner and contains the newly minted bitcoins does not reference a former output obviously. Thus, each and every "coin" can be traced back to its origin. Crucially for understanding the power of bitcoin is that inputs and outputs contain scripts. The output script defines the rules under which the value locked in this output can be spent. The input script then has to satisfy these rules. The basic output script demands a signature corresponding to a particular public key. Thus, public keys (or addresses which are derived from them) in Bitcoin are comparable to number accounts in traditional banks. However, these accounts do not have to be provided by a central authority but can be generated ad-hoc by the users themselves without any permission needed. The availability of a scripting language with cryptographic primitives is the reason why Bitcoin is sometimes called programmable money. For example many interesting applications can be designed by using multi-signature (multisig) transactions. Here an output can be spent only if m-of-n signatures are provided by the input script. This aspect of programmability can also be used to add meta data to transactions. Therefore, arbitrary data can be time-stamped and complex overlay protocols with emergent virtual chains on top of the Bitcoin blockchain can be built. We will see examples of this in the discussion of the cases in Section 5.

Nakamoto consensus has issues concerning scalability in terms of transaction throughput. In its current form the bitcoin network can handle a maximum of seven transactions per second. This limit is due to specific parameter choices in the bitcoin software and will probably be increased moderately in the coming month. This issue is currently being discussed heavily (Caffyn, 2015) under the term "blocksize debate". Because of the global peer-to-peer architecture and the finite speed of information propagation in the network there is an inherent trade off between decentralisation and transaction (Croman et al., 2016). However, the programmability allows the formation of payment channels (Bitcoin Wiki, 2015) and payment channel networks (Decker and Wattenhofer, 2015; Poon and Dryja, 2015), which alow in principle to keep most of the transactions "off-chain" and use the bitcoin network only to establish channels and for settlement. This technology also enables true micropayments in the sub-cent range. Micropayments on this order have always been prohibitive in traditional payment systems as well as with basic Bitcoin transactions because of transaction costs.

2.2 Innovation, Disruption and Disruptive Innovation

In a broader definition, innovation can be described as "the generation, acceptance, and implementation of new ideas, processes, products or services." (Thompson, 1965, p. 2). Depending on the context, the term "innovation" incorporates divergent attributes, such as different process stages or underlying constructs (Baregheh et al., 2009). Hence, the purpose of an innovation process could be to change or improve products as well as entire business models (Bucherer et al., 2012). Business models can be described as "the rationale of how an organization creates, delivers and captures value" (Osterwalder and Pigneur, 2010). Describing the logic of a company's business activities (Linder and Cantrell 2000), the business model comprises four high-level components including value proposition, operational model, financial model and customer relations. (Bucherer et al., 2012).

Depending on whether a company introduces a new service or changes its current business model, innovations can be characterized by their "degree of newness", a metric, which Garcia and Calantone (2002) describe as "Innovativeness" and "the degree of discontinuity in marketing and/or technological factors" (Garcia and Calantone, 2002, p. 112). In recent years the two notions "radical" and "disruptive" have received increased attention from scholars and practitioners alike to describe innovations with a high degree of innovativeness (Christensen et al., 2015; Latzer, 2009).

Radical innovations refer to highly discontinuous (technological) changes (Latzer, 2009) and are characterized by totally new features, high uncertainty and the necessity for companies to acquire new capabilities to fully exploit emerging opportunities (Latzer, 2009). Additionally, these often technology-driven innovations can have the potential to shift existing paradigms and might possibly disrupt industries (Latzer, 2009). Following Christensen's theory, disruptive innovation can be described as a "new product [or service] encroach[ing] on the low end of the existing market" (Schmidt and Druehl, 2008, p. 348) with the potential to move upward to satisfy higher customer expectations (Christensen, 1997, 2006). This is possible because incumbents focus on improving their offerings along performance dimensions that are valued specifically by the majority of demanding customers, while entrants focus on different performance dimensions that are (initially) valued only by niche segments, which are usually neglected by incumbents. At the same time, Christensen et al. (2015) define "disruption" as "a process whereby a smaller company with fewer resources is able to successfully challenge established incumbent businesses". Hence, a disruptive innovation does not inevitably leads to the disruption of a market, nor does a disruption of a market necessarily has to be triggered by a disruptive innovation.

The literature on disruptive innovation is currently still in an early stage (Markides, 2006) and it remains controversial, how to define the concept (Danneels, 2004; Yu and Hang, 2010). While some researchers support Christensen's understanding, contributing own thoughts to the theory, others generally "criticize the vagueness of the concept" (Yu and Hang, 2010, p. 438). According to its critics

Christensen's theorization does not allow for a clear differentiation between underperforming technologies and potentially disruptive technologies with initially inferior performance (Tellis, 2006) Finally, a main criticism focuses on the lack of measurability of disruptive innovation (Govindarajan and Kopalle, 2006). To overcome this gap, Govindarajan and Kopalle (2006), define the following criteria to identify disruptive innovations. The innovation should (1) possess inferior attributes regarding what mainstream customers would value; (2) attract new customer segments by offering new value propositions; (3) be offered at lower costs; and (4) start from niche markets (Yu and Hang, 2006; Govindarajan and Kopalle, 2006).

3 Methodology

Mapping the bitcoin ecosystem: To attain a wide dataset that adequately represents the presently existing Bitcoin start-up ecosystem, we utilized a variety of publically available online sources: The start-up platform AngelList (2015), searched with the broad keyword 'cryptocurrency', a compiled list of crypto technology companies by industry expert William Mougayar (2015) and Coindesk (2015), a reputable and well known bitcoin news site, which maintains a comprehensive list of venture capital invested into Bitcoin start-ups. To validate and add additional data to the compiled set we used the websites of the individual companies as well as press releases and the Crunchbase database (2015). We identified a total of 704 start-ups and projects in the crypto-currency and blockchain space, which are existent today. Of these, 599 belong to the Bitcoin ecosystem, and 65 received venture capital.

Following an iterative process, we identified representative categories that help understanding the Bitcoin ecosystem.

Selecting and analyzing the representative companies: Based on this classification and our focus beyond financial services, we identified six application-specific subsectors for investigation by representative case studies. The particular companies were selected based on funding and attention by the community. The case studies are grounded in a rich set of secondary data sources. Besides company websites, white papers and press releases, there are detailed founder interviews on Zapchain (2015) and Epicenter Bitcoin (2015).

Although our research approach was inherently exploratory we had two guiding questions in mind: (1) What is the core innovation of the company, and (2) on which Bitcoin features is this innovation based.

4 The Bitcoin Start-up Ecosystem

The open and permissionless nature of Bitcoin has led to a Cambrian explosion of projects and start-up companies. Table 1 provides an overview of the diversity of the ecosystem. Notably, the table is restricted to the venture-backed Bitcoin ecosystem. Projects and companies without funding as well as the growing extended ecosystem, consisting of Bitcoin-inspired alternative coins and blockchains, were not taken into account.

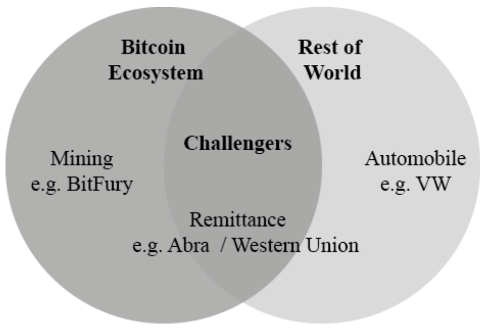

Figure 2. Distinction between challengers and the Bitcoin ecosystem without challengers.

We divide the ecosystem in two main categories (see Figure 2 for illustration). The first category consists of start-up companies that act mainly inside the Bitcoin ecosystem itself. Examples are wallet providers, mining operations and Bitcoin exchanges. We refer to this category as "Bitcoin ecosystem without challengers". Hence, the second category is termed challengers. Those are companies that use Bitcoin technology to attack traditional companies and business models outside the Bitcoin ecosystem. Examples of this category are payment processors like BitPay (2015), challenging traditional online payment processors like PayPal, and remittance services like Abra (2015), challenging incumbents like Western Union by cutting down transaction fees through disintermediation and decreased vulnerability to fraud. The classification of companies is not always clear-cut and may change as the ecosystem develops, but provides a lens to identify sectors, which might get disrupted first.

Interestingly, the challenger category is not limited to the financial service industry. We identified three main sectors beyond financial services where start-ups use Bitcoin technology to innovate and thereby challenge incumbents: (1) notary services, (2) marketplaces, and (3) digital assets. Notary services use the Bitcoin blockchain as an immutable public database and time-stamping service. Applications are records management, by providing verifiable audit trails and provable data integrity, as well as identity registries, which are not tied to a particular identity provider. Marketplaces provide a decentralized infrastructure where physical as well as digital goods and services can be traded for bitcoins. The digital assets sector is concerned with the management of "anything that exists in a binary format and comes with the right to use" (Wikipedia, 2015). This entails digital art, photographs, music, but also coupons and tickets. Furthermore, we extended the concept of digital assets to incorporate the Internet of Things (IoT), since it is concerned with the digital representation of physical devices. We will discuss these sectors in more detail by looking at representative cases in Section 5.

Figure 3. Number of new Bitcoin projects over time.

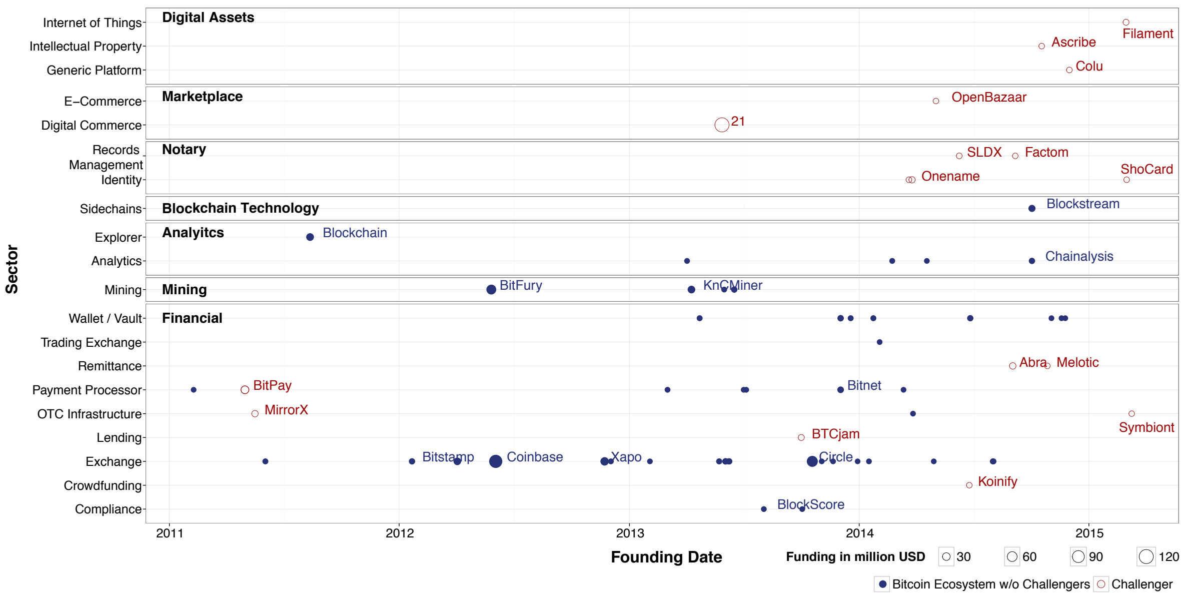

Figure 4. Evolution of the venture-backed Bitcoin start-up ecosystem.

Figures 3 and 4 give an overview of the temporal evolution of the ecosystem. Figure 3 shows the evolution of all Bitcoin projects whereas Figure 4 is restricted to the venture-backed Bitcoin start-up ecosystem. Notably, there are no companies that were founded in the first two years of Bitcoin's existence. Projects that started earlier have not survived (e.g. Mt. Gox, 2015) or have not attracted venture capital. The following three years (2011-2013) are characterized by companies building the infrastructure for the bitcoin ecosystem. From 2014 on, the number of challengers has grown, and the sectors beyond the financial sector have gained traction. Hence, these companies are very young and are just in the process of entering the market.

	Sector	Subsector	Description	Representatives	Revenue Mechanics
Challengers	Digital Assets	Internet of Things	Service to register and manage connected devices	**Filament**	Product as a Service
		Intellectual property	Service to register and manage IP like music and art	**Ascribe**, Monegraph	Transaction fee (%)
		Generic Platform	Generic platform to register and manage all kinds of digital assets	Colu, CoinSpark	Not applicable
	Marketplace	E-Commerce	Buying and selling of physical or digital products	**OpenBazaar**	Not applicable
		Digital (micro) Commerce	Buying and selling digital micro services like individual API usage	**21**	Device sales (currently)
	Notary	Records Management	Service to provide data integrity and auditability	**Factom**	Token sale
		Identity	Service to provide an identity to authenticate across the Intern	**Onename**, Shocard	Not applicable
	Financial	Payment processor	Payment services for merchants	BitPay, Coinbase	Transaction fee (%)
		Remittance	Global transfer of money across boarders	Abra	Flat fee for depositing/withdrawing funds
		OTC Infrastructure	Infrastructure to trade commodities, financial instruments, and derivatives	Symbiont, Mirror	Project based
		Lending	Service to facilitate peer-to-peer lending	Bitbond	Transaction fee (%)
		Crowdfunding	Service to facilitate crowdfunding for projects	Koinify, Swarm	Transaction fee (%)

Bitcoin Ecosystem without Challengers	Blockchain Technology	Sidechains	Technology for custom blockchains compatible with bitcoin	Blockstream	Project based
	Analytics	Analytics	Service for browsing and analyzing blockchains	Coinalytics, Blockchain	Project based
	Mining	Mining	Manufacture and/or operating mining infrastructure	BitFury, KnC Miner	Bitcoin mining, device sales
	Financial	Wallet / Vault	Product or service to store private keys, and optionally initiate transactions	Case, Xapo, Coinbase	Ancillary services
		Exchange	Service to trade bitcoins for other currencies	Bitstamp, Kraken, Gem	Transaction fee (%)
		Compliance	Service to provide KYC and AML compliance[1]	Elliptic, BlockScore	Transaction fee (%)

Table 1. A categorization of the (venture-backed) Bitcoin start-up ecosystem.

5 Case Studies

In the following, we investigate the challengers beyond financial services in more detail. Therefore, we present six comprehensive case studies (marked bold in Table 1).

5.1 Filament (Internet of Things)

Filament (2015) provides wireless sensor networks for the (industrial) IoT, e.g. for smart cities or smart agriculture use case. Most IoT platform providers follow a centralized approach by connecting all devices to their respective cloud-infrastructure. This has the major disadvantage that devices depend on a central infrastructure in order to operate. Moreover, it can be argued that this approach cannot keep up technically and economically with the increasing number connected devices.

Filament is one of the first companies that develop a fully decentralized IoT infrastructure, which encompasses three blockchain-related aspects: (1) Each device is registered on the blockchain providing a verifiable and immutable identity. This enables discovering of and authenticating with other devices/services without the need of a dedicated backend infrastructure. Therefore, devices are technically autonomous and are able to operate independently of Filament. (2) Each device is governed by a "smart" contract, which manages agreements of device control/ownership, data access and financial agreements concerning the device. Ownership can be transferred permanently or temporarily by a simple transaction on the blockchain. Filament implements the financial agreements as a Product-as-a-Service, which means that the owner gets paid directly for the ongoing use of the device. (3) Furthermore, each device is able to transfer value in form of bitcoins to other devices in order to get access to data or request some service.

As described, devices can be operated and governed by using only the blockchain as a backend and therefore without any technical dependence on the platform creator (Filament) or other third parties. This might bare great benefits for customers needing to deploy large Industrial IoT applications with a lifetime of 5-10 years. Because they want to minimize the risk of a lock-in with a specific company. Moreover, according to Filament, customers prefer paying continuously on a real-time basis instead of an upfront investment, which can be solved efficiently by Bitcoin micropayments. Ownership is decoupled from usage and both are independent of the manufacturer or a platform provider.

Filament itself is a venture capital-backed company formerly known as Pinocc.io. They claim to have their first deployments with Fortune 500 companies in 2016. They will get paid for the ongoing use of their devices (by owning the smart contract). Moreover, they work on a licensing model, i.e. Customers can attach a module version to their own devices, which will give them all the described benefits of

[1] KYC: Know your customer. AML: Anti money laundering. Both are bank regulations

Filament in return to a small fraction of the payments for the ongoing use of the devices. However, since all protocols will be open and there is no dependence to Filament by design, other companies could use that and build their own hardware without Filament.

5.2 Ascribe (Intellectual Property)

Ascribe (2015) aims to provide provenance of intellectual property. Digital work, like art, photos, and music, can be registered publicly on the bitcoin blockchain together with its accompanying terms and conditions. The technological basis is the spool protocol (De Jonghe and McConghy, 2015), an overlay protocol that uses Bitcoin transactions to represent unforgeable ownership transfers and licensing agreements for digital work. Thus, authenticity of ownership and usage rights can always be proven. Ascribe focuses on digital art in particular. Although art is in principle copyrighted by the time of creation, it is currently cumbersome and expensive to officially register work and prove ownership (see e.g. http://copyright.gov/docs/fees.html). Therefore, hardly any digital art gets registered. Ascribe aims to change the status quo by providing a virtually free and automatable registration process. Moreover, the unique representation of digital work based on cryptography and the blockchain is the basis for the creation of a secondary market for digital work. For example the spool protocol enables creating limited editions of digital work. So far, this has not been possible without relying on some central institution.

The spool protocol is open source and can be used by anybody. In principle, the only costs are bitcoin transaction fees. However, Ascribe wraps the protocol in convenient web services and provides tools adapted to particular customer groups, e.g. individual creators, museums and marketplaces. Ascribe's revenue model is then based on a share of the rentals and sales of registered digital work that are facilitated by their APIs.

The core innovation is the application of the bitcoin blockchain to provide commoditized provenance of intellectual property. Provenance is demonstrated by relying on the immutability of the bitcoin blockchain, instead of an authority.

5.3 OpenBazaar (E-Commerce Marketplace)

OpenBazaar (2015) is an open source project consisting of a protocol and a reference implementation that enables a decentralized peer-to-peer e-commerce marketplace. In comparison to traditional e-commerce market places like eBay and Amazon, there is no central server or authority that is running the market place. Thus, there is no middleman who is able to charge fees or to restrict offered products and services. Everyone with Internet access is able to set up a shop by running a network client. Payments are facilitated using Bitcoin transactions. Therefore, no payment provider or banking account is needed. This lowers payment transaction fees and increases the global reach. Besides sellers and buyers there are notaries and arbiters for dispute resolution participating in the marketplace. Those latter participants are involved by using bitcoin multi-signature transactions. Thus, OpenBazaar unbundles the functions of traditional marketplaces. Trades on the OpenBazaar network are based on Ricardian Contracts (Grigg, 2004), i.e. an electronic document that defines the terms of a trade such that it is readable by computers and humans, and is cryptographically signed. Apart from selling physical and digital products, OpenBazaar can also be used to trade speculative contracts, which can be readily represented by Ricardian Contracts.

The main value proposition of OpenBazaar to sellers as well as to buyers is the elimination of fees and restrictions. Since marketplaces are subject to network effects most users will most probably not switch immediately from traditional marketplaces to OpenBazaar. However, OpenBazaar could set foot in under-served niche markets. Examples could be digital goods, developing countries with limited access to traditional payment services, and prohibited goods.

OpenBazaar itself is not a company, but its main developers founded the venture capital-backed company OB1. Their current focus is on developing the OpenBazaar protocol and its reference implementation. As outlined above, OB1 is not able to profit directly from transactions on the marketplace in the way traditional revenue mechanics on centralized marketplaces work.

5.4 21 (Digital Micro Commerce Marketplace)

At first sight, the categorization of 21 Inc. (2015) as a challenger seems odd, since 21 is an infrastructure and platform provider for the bitcoin ecosystem. Indeed, it is often categorized as a mining company. However, we argue that 21 is better classified as a marketplace for digital micro services, which has the potential to challenge traditional Internet business models.

With a funding of $121M, 21 supersedes every other start up in the bitcoin ecosystem. They have developed an embeddable ASIC[2] mining chip that they are using in their own mining operations, but which is also embeddable into arbitrary connected devices. In November 2015 they released their first product, the 21 Bitcoin computer. Essentially the 21 Bitcoin computer is a full-stack development platform to build bitcoin-payable digital services, which can be published and discovered on 21's digital marketplace. Individual service consumptions, like an API call, can be billed at as little as 1 satoshi[3]. The embedded mining chip, which is currently coupled to a mining pool (Antonopoulos, 2014, pp. 209-211) operated by 21, supplies the device with a continuous stream of satoshis.

21 aims to embed their chips into any connected device (e.g. smart phones) to establish bitcoin as a system resource like CPU, bandwidth or disk space, but for the purpose of buying and selling digital goods and services (Srinivasan, 2015). It is crucial to understand that it does not make sense to sell the small amounts of mined bitcoins for Fiat currency on an exchange. Instead, the idea is to supply every device with a continuous stream of bitcoin from the point of commissioning on so that it can directly operate on the marketplace.

Having such an infrastructure of bitcoin-enabled devices in place at scale, could offer compelling new opportunities and even disrupt traditional business models of the Internet. For example, it has been difficult for news sites to directly monetize their content on the Internet. It is still tedious for users who want to read just one article to signup, enter their credit card information and buy a subscription. Thus, most news sites still depend on indirect revenue by advertisements, which becomes more problematic with the increasing spread of ad-blockers. These problems could be eliminated with the diffusion of a bitcoin-enabled infrastructure for frictionless micropayments. Similarly, a bitcoin-enabled IoT device, e.g. for automatic irrigation of farms, could pay a weather service API in return for accurate weather prediction data without the need for signup. Moreover, the device could search automatically for the cheapest (and best in terms of reputation) weather service API on the marketplace.

The 21 platform is a mixture of a centralized and a decentralized model. As of today, the mining power is bound to 21, and returns get allocated to a wallet owned by 21. However, it is announced that this will change in the future. The marketplace for digital services on the other hand is in principle decentralized and trades can be conducted peer-to-peer. Currently, 21 generates revenue by private mining operations and by sales of the bitcoin computer. In the future, however, all kinds of interesting revenue models are imaginable: selling and licensing of mining chips, revenue sharing of embedded mining operations or tiny transaction fees for off-chain transactions to name just a few.

In conclusion, 21 could change how resources in the Internet are paid for, and thereby also contribute to making new resources available, which have not been available yet because of missing incentives

[2] Application-specific integrated circuit. A hardware chip customized for a particular task in contrast to a general CPU. In this case task is Bitcoin mining, which involves the extensive execution of SHA265 operations.

[3] Satoshi is the smallest denominator of a bitcoin. 100,000,000 satoshi correspond to 1 bitcoin. Thus, 1 satoshi is currently worth approximately USD 0.000003.

5.5 Factom (Records Management)

Factom (2015) is an open source software project that provides businesses with the ability to prove data integrity and to create verifiable and immutable audit trails.

While data integrity could be achieved by directly adding a hash of the data to a bitcoin transaction and thereby time-stamp the data on the bitcoin blockchain, this method does not scale. On one hand, this is because of inherent scalability issues of bitcoin, and on the other hand because of transaction fees. Therefore, Factom consists of a peer-to-peer network that is independent of the bitcoin network. Customers of Factom generate hashes of their data and send them for recordkeeping to the Factom network. There, all hashes are compressed to a single hash by building a Merkle tree (Merkle, 1980) and taking the root of the tree. This single hash value is then stored in the bitcoin blockchain. This provably time-stamps all individual records without having to write all records individually into the bitcoin blockchain. The network maintains its own crypto-currency, "factoids", which is used to incentivize participants of the peer-to-peer network to provide their resources. A factoid can be transformed into entry credits, which can be used to submit new records. The price of a factoid depends on the market value, but the price of an entry credit is fixed to $1/10^{th}$ of a cent.

In summary, Factom provides a decentralized platform for data provenance with a permanent, time-stamped record of an unforgeable reference to the data anchored in the blockchain. This offers an efficient and cheap alternative for businesses, institutions and governments to have a proof of existence, proof of process or proof of audit for their data. Their first publicly announced project is using Factom for an official land title registry in partnership with the government of Honduras (Chavez-Dreyfuss, 2015). In fact, Factom is an interesting option for governments in developing countries. They often face mismanagement and corruption, but cannot afford or enforce infrastructure and processes to guarantee compliance of their administration. Moreover, the Factom solution offers also an opportunity for small businesses/start-ups to have more auditing and to prove compliance with regulations without hiring expensive professional companies for that.

5.6 Onename (Identity)

Onename (2015) allows registering identities on the Bitcoin blockchain. This blockchain identity can be connected to various online identities like Facebook, Twitter, PGP keys and a Bitcoin address. Thus, it provides a probabilistic identity which reliability grows with the number of verified connected accounts. Onename is based on an open source overlay protocol called Blockchain ID. Everyone is able to register his identity without having to rely on Onename services. Blockchain identities are independent of the company Onename, are referenced on the Bitcoin blockchain and are therefore owned by the holder of the respective private key.

Blockchain IDs will allow signing up on third party websites comparable to Facebook Login or Google Sign-In. There is no need for passwords since authentication is done using digital signatures. Blockchain ID is also used as an identity provider for OpenBazaar.

Moreover, it is possible to add additional namespaces. In this sense Blockchain IDs could represent not only humans, but also machines. Thus, Blockchain IDs might be the basis of a decentralized DNS system or an IoT registry.

Essentially, the technology allows individuals to own their online identities, rather than being dependent central institutions. Holding, i.e. registering and prolonging, a Blockchain ID requires fees that directly support the Bitcoin ecosystem. One part of the fee is a typical Bitcoin transaction fee that will be collected by a miner. The other part of the fee is particular to the protocol and leads to "burning" of bitcoins. Since the number of bitcoins is constrained, the elimination of bitcoins theoretically increases the value of existing bitcoins. While it might seem that our current identities are free, we actually pay with our personal data. Every time we use Facebook to login into a third party website, we give away more information about us. Identity is also subject to network effects. Institutions will only start to accept Blockchain IDs if there are enough people using them and demand acceptance.

Onename basically follows the same strategy as OB1. The initial focus is on developing open source protocols and advocating their adoption, instead of having a revenue model in place.

6 Key Findings

Table 2 presents the key findings concerning our main research questions. We state the core innovation of the company in the respective sector and list the features of Bitcoin that underlay those innovations. The innovations in the digital asset sector and in the notary sector are enabled mainly because of the usage of the Bitcoin blockchain as an immutable public database. In contrast, the decentralized marketplaces profit from the value transfer features Bitcoin provides, in particular multi-signature escrow and micropayments. Both features are ultimately based on the scriptability of Bitcoin transactions, i.e. the nature of Bitcoin as programmable money. Another important aspect that encompasses all sectors is the inclusivity and permissionless nature of Bitcoin. This aspect has two implications. First, it allows companies to build protocols on top of Bitcoin and the blockchain without having to ask anyone for permission. All of the presented companies are based on this. Second, everyone with Internet-connectivity is able to participate in the system. In particular, people from developing countries without proper access to financial services can be active on the marketplaces.

Rather surprising is the appearance of mining. The business model of traditional mining operations is to generate revenue by selling newly minted bitcoins. In contrast, 21 aims to leverage mining as a tool to supply users directly with bitcoins circumventing the cumbersome process of acquiring those on an exchange. Thus fuelling the emerging ecosystem of bitcoin-payable digital micro services.

Sector	Subsector	Company/ Project	Core innovation	Bitcoin features				
				Immutable public database	Inclusive (global and permissionless)	Mining	Micro-payments	Multisig
Digital Assets	Internet of Things	Filament	Decentralized IoT infrastructure based on autonomous devices	✔	✔		✔	
	Intellectual Property	Ascribe	Commoditization of registering IP; trade and license digital work	✔	✔			
Marketplace	E-Commerce Marketplace	OpenBazaar	Decentralized market place for physical and digital goods without restrictions and fees		✔			✔
	Digital Micro Services Marketplace	21	Ecosystem for bitcoin-payable digital (micro) services		✔	✔	✔	
Notary	Records Management	Factom	Commoditizing data integrity and auditability	✔	✔			
	Identity	Onename	Individually-owned identities	✔	✔			

Table 2. Results of the case studies: Core innovations and underlying Bitcoin features.

7 Discussion

In the title of this work we stated the question on whether the Bitcoin ecosystem may disrupt sectors beyond the financial service industry. We would argue that the companies we investigated in this paper are leveraging Bitcoin as global programmable money and as an immutable public database to foster radical innovations in their respective sectors. Central authorities are eliminated and new markets are created. But as shown in Section 2.2 radical innovations are not necessarily disruptive innovations and disruptive innovations may or may not disrupt a market eventually. Thus "identifying disruptive innovation is a complex process" (Kaltenecker et al., 2015). The current literature still lacks a thorough theoretical foundation, on how to define disruptive innovations (Yu and Hang, 2010). Additionally it remains unclear to what degree disruptive innovations can be predicted ex ante (Barney, 1997; Tellis, 2006). This article aims to offer an overview on the fast developing blockchain ecosystem highlighting mainly the potential inherent to these technologies. Most sectors that we considered are underdeveloped. The commoditization of registration of digital work and intellectual property in general could be counted as a new-market disruptive innovation. Current registration of IP is expensive and cumbersome, but is backed directly by jurisdiction. Therefore, in terms of legal certainty, the traditional process is clearly superior. Decentralized marketplaces exhibit also the characteristics of a disruptive innovation. Today, OpenBazaar has an inferior user experience in comparison to Amazon or eBay. Moreover, it obviously does not have the same strong user base. However, the OpenBazaar platform is free to use and there are no restrictions on what can be sold. These characteristics will most probably attract users in niche segments and could grow from there on. In cases like Filament and Onename the notion of disruptive innovation does only apply to a lesser extend. Interestingly, most of the core innovations that the companies provide are in form of open source protocols. Thus, the disruptive potential is not entirely dependent on the future of the particular companies. From the point of the start-ups, open source protocols and decentralization can help entering a market that is dominated by a central institution. However, it becomes much harder to capture value and thus to find a sustainable business model.

As shown in Figure 4, most of the ecosystem beyond financial services is younger than two years. The companies are in a very early stage and the focus is clearly on creating value and on advocating the use of their protocols. Some of the companies are experimenting with ways to capture value. But it is too early to investigate the business model in detail. Noteworthy, all of the six start-ups under consideration build platforms. In fact, these platforms are rather different. For example Filament builds a decentralized platform for the Internet of Things, Onename builds a decentralized identity layer and so on and so forth. Hence, it will be worthwhile to study the emergent value networks as soon as the platforms get populated.

Despite these first insights, more research will be required to gain a better understanding of the theory of disruptive innovation in general, as well as in the context of blockchain technologies in particular (cf. Danneels, 2004). We encourage other scholars to take this article as a starting point to investigate more precise measurements (cf. Govindarajan and Kopalle, 2006) and clearer definitions (cf. Markides, 2006) of disruptive innovation in a Fintech context as well as to draw clear distinctions to related research fields such as radical or open innovation (cf. Yu and Hang, 2010).

In this work, we deliberately restricted our scope on start-up companies building on Bitcoin technology. However, there are numerous implementations of cryptocurrencies and blockchains. While most of them are mere copies with different parameter choices, there are also developments with the potential to advance the technology and applications significantly. Most notably there is Ethereum, which e.g. replaces the restricted scripting language of Bitcoin with a Turing-complete programming language that allows programs "living" on the Ethereum blockchain, so called contracts, to govern over funds autonomously. This empowers developers to build richer decentralized applications on top of the (Ethereum) blockchain. The Ethereum network launched as recently as July 2015 and has still to prove its resilience. Thus far, there are hardly any venture-backed companies in sectors beyond financial services that use alternative cryptocurrencies and blockchains. However, this might change soon.

Acknowledgements

The present work is supported by the Bosch IoT Lab at the University of St. Gallen, Switzerland.

References

21 (2015). URL: https://21.co/ (visited on 25/11/2015)

Abra (2015). URL: https://www.goabra.com/ (visited on 25/11/2015)

AngelList (2015). URL: https://angel.co/cryptocurrency-2 (visited on 30/09/2015)

Antonopoulos, A. M. (2014). *Mastering Bitcoin: unlocking digital cryptocurrencies*. „O'Reilly Media, Inc.".

Ascribe (2015). URL: https://www.ascribe.io/ (visited on 25/11/2015)

Back, A. (2002). Hashcash-a denial of service counter-measure.

Baiyere, A., Donnellan, B., Hevner, A., Smith, C., & Stikeleather, J. (2015). „Disruptive Innovations and IT - Wicked yet Empowering combination.“ In: *Proceedings Thirty Sixth International Conference on Information Systems*

Baregheh, A., J. Rowley J. and S. Sambrook (2009). “Towards a multidisciplinary definition of innovation”. *Management Decision* 47 (8), 1323–1339.

Bitpay (2015). URL: https://bitpay.com/ (visited on 25/11/2015)

Bitcoin Wiki (2015). Example 7: Rapidly-adjusted (micro)payments to a pre-determined party. URL: https://en.bitcoin.it/w/index.php?title=Contract&oldid=59172#Example_7:_Rapidly-adjusted_.28micro.29payments_to_a_pre-determined_party (visited on 27/11/2015)

Bucherer, E., U. Eisert and O. Gassmann (2012). *„Towards Systematic Business Model Innovation: Lessons from Product Innovation Management”*. Creativity and Innovation Management 21 (2), 183–98.

Caffyn, G. (2015). What is the Bitcoin Block Size Debate and Why Does it Matter?. URL: http://www.coindesk.com/what-is-the-bitcoin-block-size-debate-and-why-does-it-matter/ (visited on 27/11/2015)

Chain (2015). URL: http://chain.com/ (visited on 25/11/2015)

Chavez-Dreyfuss, G. (2015). *Honduras to build land title registry using bitcoin technology*. URL: http://in.reuters.com/article/2015/05/15/usa-honduras-technology-idINKBN0O01V720150515/ (visited on 25/11/2015)

Christensen C.M. (1997). *The Innovator‘s Dilemma When New Technologies Cause Great Firms to Fail*. Cambridge, Mass: Harvard Business School Press.

Christensen, C.M. (2006). „The Ongoing Process of Building a Theory of Disruption“. *Journal of Product and Innovation Management* 23, 39-55.

Christensen, C.M., M. E. Raynor and R. McDonald (2015). “What is Disruptive Innovation?“. *Harvard Business Review* 87 (2), 43-49.

Coindesk (2015). *Bitcoin Venture Capital*. URL: http://www.coindesk.com/bitcoin-venture-capital/ (visited on 8/10/2015)

Crunchbase (2015). URL: https://www.crunchbase.com/ (visited on 25/11/2015)

Danneels, E. (2004). Disruptive technology reconsidered: A critique and research agenda. *Journal of product innovation management*, 21(4), 246-258.

De Jonghe D. and T. McConaghy. (2015). *Spool.* URL: https://github.com/ascribe/spool (visited on 27/11/2015)

Decker, C. and R. Wattenhofer. (2015). „A fast and scalable payment network with Bitcoin Duplex Micropayment Channels“. In *Stabilization, Safety, and Security of Distributed Systems* (pp. 3-18). Springer International Publishing.

Douceur, J. R. (2002). The sybil attack. In *Peer-to-peer Systems* (pp. 251-260). Springer Berlin Heidelberg.

Dougherty C. and G. Huang (2014). *Mt. Gox Files for Bankcruptcy After $470 Million Bitcoin Loss.* URL: http://www.bloomberg.com/news/articles/2014-02-28/mt-gox-files-for-bankruptcy-after-470-million-bitcoin-loss/ (visited on 25/11/2015)

Epicenter Bitcoin (2015). URL: https://epicenterbitcoin.com/ (visited on 25/11/2015)

Ethereum (2015). URL: https://www.ethereum.org/ (visited on 25/11/2015)

Factom (2015). URL: http://factom.org/ (visited on 25/11/2015)

Filament (2015). URL: www.filament.com (visited on 25/11/2015)

Garcia, R. and R. Calantone (2002). „A critical look at technological innovation typology and innovativeness terminology: a literature review". *Journal of product innovation management* 19 (2), 110-132.

Giaglis, G. M. and K. N. Kypriotaki (2014). „Towards an Agenda for Information Systems Research on Digital Currencies and Bitcoin". In *Business Information Systems Workshops* 183 (pp. 3–13). Cham: Springer International Publishing. http://doi.org/10.1007/978-3-319-11460-6_1

Glaser, F., Zimmermann K., Haferkorn M., Weber M. and Siering M. (2014). „Bitcoin – Asset or Currency? Revealing Users' Hidden Intentions." In: *Proceedings of the European Conference on Information Systems*

Glaser, F. and Bezzenberger, L. (2015). „Beyond Cryptocurrencies - A Taxonomy of Decentralized Consensus Systems." In: *Proceedings of the European Conference on Information Systems*

Govindarajan, V., & Kopalle, P. K. (2006). The Usefulness of Measuring Disruptiveness of Innovations Ex Post in Making Ex Ante Predictions. *Journal of product innovation management*, 23(1), 12-18.

Grigg, I. (2004). „The ricardian contract." In *Electronic Contracting, 2004. Proceedings. First IEEE International Workshop on* (pp. 25-31). IEEE.

Huy, Y., Jeon, S., and Yoo, B. (2015). „Is Bitcoin a Viable E-Business?: Empirical Analysis oft he Digital Currency's Speculative Nature." In: *Proceedings Thirty Sixth International Conference on Information Systems*

Ingram, C., Morisse, M., and Teigland, R. (2015). „A Bad Apple Went Away: Exploring Resilience among Bitcoin Entrepreneurs." In: *Proceedings of the European Conference on Information Systems*

Kaltenecker, N., Hess, T., and S., Huesig (2015). Managing potentially disruptive innovations in software companies: Transforming from On-premises to the On-demand. *The Journal of Strategic Information Systems*, 24(4), 234-250.

Kazan, E., C-W Tan and E. T.K. Lim (2015). „Value Creation in Cryptocurrency Networks: Towards A Taxonomy of Digital Business Models for Bitcoin Companies". In: *PACIS 2015 Proceedings.* Paper 34. http://aisel.aisnet.org/pacis2015/34

Lamport, L., R. Shostak and M. Pease (1982). „The Byzantine generals problem". *ACM Transactions on Programming Languages and Systems* 4 (3), 382-401.

Latzer, M. (2009). Information and communication technology innovations: radical and disruptive?. *New Media & Society* (Vol. 11.4, pp. 599-619).

Markides, C. (2006). Disruptive innovation: In need of better theory. *Journal of product innovation management*, 23(1), 19-25.

McGullagh, D. (2001). *Digging those DigiCash blues*. URL: http://www.wired.com/2001/06/digging-those-digicash-blues/ (visited on 11/17/2015)

Merkle, R. C. (1980). „Protocols for public key cryptosystems". In *Proc. IEEE Symp. Security Pri*vacy. pp. 122 -134. IEEE.

Morisse, M. (2015). „Cryptocurrencies and Bitcoin: Charting the Research Landscape." In: *Proceedings Twenty-first Americas Conference on Information Systems*

Mougayar, W. (2015). *Crypto-Technology Landscape.* URL: http://crypto.silk.co/ (visited on 2/10/15)

MtGox (2015). URL: https://www.mtgox.com/ (visited on 25/11/2015)

Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system.

Onename (2015). URL: https://onename.com/ (visited on 25/11/2015)

OpenBazaar (2015). URL: https://openbazaar.org/ (visited on 25/11/2015)
Osterwalder, A. and Y. Pigneur (2010). *Business model generation: a handbook for visionaries, game changers, and challengers*. John Wiley & Sons
Ripple (2015). URL: https://www.ripple.com/ (visited on 25/11/2015)
Poon J. and T. Dryja (2015). „*The bitcoin lightning network*". URL: https://lightning.network/lightning-network-paper.pdf / (visited on 25/11/2015)
Schmidt, G. M. and C. T. Druehl (2008). „When Is a Disruptive Innovation Disruptive?*". *Journal of Product Innovation Management* 25 (4), 347-369.
Srinivasan, B. S. (2015). *A bitcoin miner in every device and in every hand.* URL: https://medium.com/@21/a-bitcoin-miner-in-every-device-and-in-every-hand-e315b40f2821#.ia1hdgz1w (visited on 27/11/2015)
Tellis, G. J. (2006). Disruptive technology or visionary leadership?. *Journal of Product Innovation Management*, 23(1), 34-38.
Wikipedia (2015). Digital Asset. URL: https://en.wikipedia.org/wiki/Digital_asset
Yu, D., and C. C., Hang (2010). A reflective review of disruptive innovation theory. *International Journal of Management Reviews*, 12(4), 435-452.
Zapchain (2015). URL: https://www.zapchain.com/ (visited on 25/11/2015)