Blockchain Implications for Marketing; A Review and an Empirical Analysis

Taher M. Al-Ahwal

Department of Corporate Economy, Faculty of Economics and Administration, Masaryk University, Brno, Czech Republic. E-mail: 490977@mail.muni.cz

Dušan Mladenović 🆔

Assistant professor, Department of Corporate Economy, Faculty of Economics and Administration, Masaryk University, Brno, Czech Republic. E-mail: dusan.mladenovic@econ.muni.cz

Ahad ZareRavasan *🆔

*Corresponding Author, Assistant professor, Department of Corporate Economy, Faculty of Economics and Administration, Masaryk University, Brno, Czech Republic. E-mail: Zare.Ahad@mail.muni.cz

Abstract

Blockchain technology was initially implemented for cryptocurrencies in 2009, but it caught the undivided attention of multiple industries such as finance, supply chain management, healthcare, and governments. This research was set out to investigate and evaluate six benefits of blockchain for marketing: fostering disintermediation, combating click fraud, reinforcing trust and transparency, enhancing privacy protection, empowering digital marketing security, and enabling creative loyalty programs. An empirical study in the form of an online survey was conducted to examine the realization of benefits in practice. The research concluded that blockchain does indeed provide promising benefits for marketing, but that depends on whether marketers use public (permissioned) blockchain or private (permissioned) blockchain, and also the ability of the blockchain community to resolve fundamental challenges and pending issues such as scalability, speed, interoperability, and privacy, besides several many others.

Keywords: Blockchain; decentralization; disintermediation; immutability; marketing.

Introduction

For decades, the world's financial transactions and data flow have been facilitated and controlled by third-party "trusted" institutions–intermediaries–such as banks, governments, and large corporations. Many believe the 2008 financial crisis proved that many of these institutions were not worthy of such trust and a change is inevitable. In the same year of the crisis, an anonymous entity named Satoshi Nakamoto (2008) published a white paper called Bitcoin: A Peer-to-Peer Electronic Cash System. It proposed an effective blockchain-based mechanism that allows for secure and direct exchange of transactions using digital money (cryptocurrency) across borders without intermediaries' intervention or verification. However, the potentials of blockchain go beyond bitcoin and financial applications. Some believe that blockchain is shifting the internet from a medium of publishing information to an internet of value. Tapscott and Tapscott (2016) propose what if there were an 'Internet of value,' some global distributed ledger or database where anything of value, from money to music to votes, could be managed, transacted, and exchanged privately and securely. They elaborate that blockchain is a transactional platform that will enable the "fourth industrial revolution" technologies (e.g., artificial intelligence, Internet of Things (IoT), drones) to be part of a more valuable economy (Kirkland & Tapscott, 2017). Others go even farther by asserting that blockchain is not merely a disruptive technology but a new paradigm—after the mainframe computer, the PCs, the World Wide Web, and the social media— that will have a significant impact upon our society because of its envisaged prospects in reshaping the digital economy as a whole (Swan, 2015). Casey and Vigna (2018) also propose that the need for trust and intermediaries allows behemoths such as Google, Facebook, and Amazon to turn economies of scale and network effects into de facto monopolies. So, if blockchain can remove the need for trust and intermediaries, then a completely new ecosystem is foreseen.

The unique characteristics of the blockchain (decentralization, distribution, immutability, and tokenization) caught the attention of many industries that saw invaluable business benefits beyond cryptocurrencies in this novel technology. A few years after Bitcoin came into existence, lots of industries invested heavily in various blockchain-based applications. Furthermore, the research community (e.g., consulting companies, educational institutions, independent researchers) has conducted researches about blockchain's impact on many of those industries (e.g., Bamakan et al., 2021; McGhin et al., 2019; Min, 2019; Saberi et al., 2019; ZareRavasan et al., 2021). However, there is limited research about blockchain's impact on marketing. Therefore, this research aims to comprehensively review theoretical and practical aspects of blockchain in the marketing industry and empirically examine it.

Blockchain in marketing

The marketing industry is no different from other industries that found promising benefits in the blockchain. Harvey et al. (2018) suggest that since most blockchain applications have been focused on finance, the technology has been mainly under the radar screen in marketing.

We argue that blockchain has an impact on the practice of marketing. There are potentially large rewards for the early adopters in marketing – and costs for those left behind by this innovation. Blockchain is predicted to solve significant problems that have haunted marketers and brands for quite some time. According to a recent report, ad fraudulent, for example, cost global advertisers approximately US$19 billion in 2018. This figure represents 9% of the total marketing budget spent on digital advertising. The study indicates that fraud ads will reach $44 billion by 2022 (BusinessWire, 2017). With blockchain's features like disintermediation, transparency, and immutability, not only can marketers and brands avoid ad frauds and save money, but also build a strong connection with their customers, regain their trust and loyalty, and design more effective marketing campaigns and long-term strategies based on direct communication with consumers.

Blockchain is set out also to benefit consumers in many ways, including data privacy. The more consumers engage in social media and e-commerce, the higher chances their privacy is breached. Facebook, for example, is facing mass legal actions for failing to protect the personal data of 87 million of its users. This company is accused of sharing users' data with Cambridge Analytica — a political consultancy — for advertising purposes during elections. In a blockchain platform, a user's identity is pseudonymous; therefore, it is almost impossible to violate users' privacy. Through the use of blockchain, consumers have full control of their data, thereby getting paid for surrendering their identity to brands and viewing their ads (Harvey et al., 2018). Blockchain is also considered an innovative tool to reform loyalty programs and enhance users' experience.

In general, the research on blockchain in marketing is in its early stages. In the past few years, marketing and academic researchers merely touched this technology to explore possible applications for marketing. Antoniadis et al. (2019) presented a mind-map derived from analysis and postings of many websites and blogs that illustrate vast applications of blockchain-in-marketing (Figure 1).
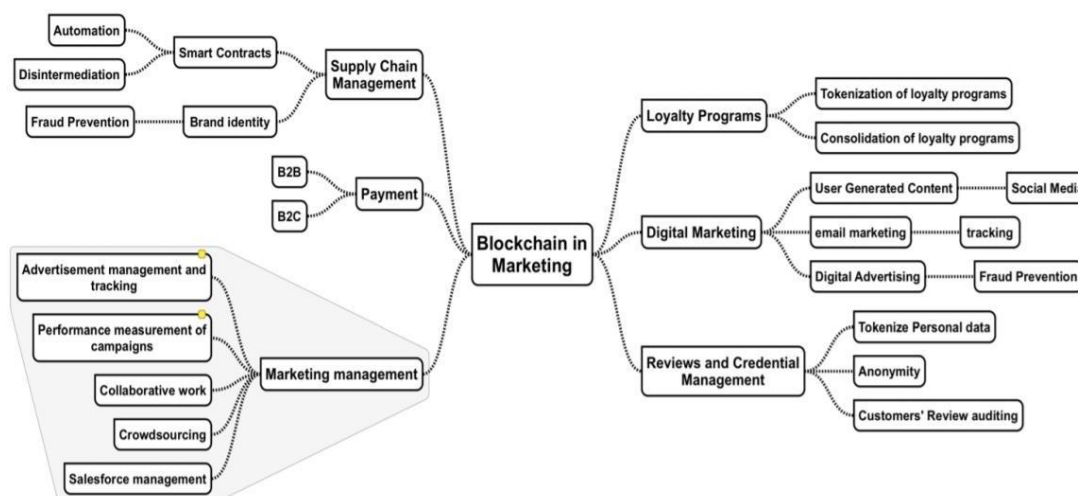

Figure 1. Mind-map of applications of blockchain in marketing (Antoniadis et al., 2019).

Antoniadis et al. (2019) also listed the six areas (or benefits) of blockchain in marketing: 1) fostering disintermediation; 2) combating click fraud; 3) reinforcing trust and transparency; 4) enhancing privacy protection; 5) empowering digital marketing security; and 6) enabling creative loyalty programs. Further explanation is presented in the following sub-sections.

Fostering disintermediation

Disintermediation is the disappearance of a wide variety of 'middlemen,' or intermediaries, and the creation of an enhanced sales network in which customers deal directly with service providers (Jallat & Capek, 2001). The advent of the internet formulated a new type of intermediation, called re-intermediation. Re-intermediation is partially removing the intermediation layers and replacing traditional intermediaries with digital ones (or e-intermediaries) (Rosenbloom, 2007), such as Google, Facebook, Alibaba, Amazon, eBay, Airbnb, and Uber. These e-intermediary titans may not share the same business model, but they all contributed significantly towards a more customer-centric digital environment where communication and interaction between buyers and sellers have become easier, faster, more economic, and indeed more engaging than ever before. However, that, unfortunately, comes with a high cost. Not only do e-intermediaries monetize consumers' personal information, shopping habits, and interaction history data, but they also chop off a portion of the transaction value. Most of these businesses are highly dependent on the content created by parties interacting on their platforms. Because of its decentralization nature, blockchain can foster true disintermediation and enable content creators to fully reap the harvest of their creation that e-intermediates have precluded. Bypassing those e-intermediaries can therefore furnish the following benefits.

First, it can forge stronger relationships between consumers and brands, which helps brands to know their customers better, encourages customer engagement, and drives more relevant campaigns (Antoniadis et al., 2019). Second, it can result in reduced intermediation costs. Uber, for example, incurs 25% from each ride. Content creators or service providers (the drivers) lose a big chunk of the value. With blockchain, this could probably end. The start-up La'Zooz, for example, established a blockchain network in which drivers can directly share rides and earn tokens in the network. Third, cutting intermediation costs could be considered crucial for marketers as digital ads costs have proven super expensive. From the $563 billion global spending in marketing in 2019 alone, half of it was on digital ads through e-intermediaries (Khan & Kushwah, 2021). Several blockchain start-ups have therefore emerged recently to tackle this issue. SaTT (Smart Advertising Transaction Token), for instance, is a blockchain platform that adopts an influencer advertising strategy to enable social media users to become influencers for a particular brand. The reward is SaTT's tokens that are cashable. This direct interaction between advertisers and content creators reduces the cost for advertisers and benefits content creators. This multiple-benefit transaction strengthens the relationship between the two parties, encourages more interaction, and develops greater

commitment from both sides. Another blockchain-based start-up, Steemit, uses a similar principle of rewarding content creators and ad viewers through fostering disintermediation (Ertemel, 2018).

Combating click fraud

Pay-per-click (or PPC) is when a user clicks on an ad that appears on a publisher's website, and the ad agency is charged per click. PPC is one of the most common methods of online advertisement. It, however, has faced a significant problem, click fraud. Click fraud uses computer programs —known as bots— (or humans) to repeatedly click on the ads to generate fake traffic and consume the ad budget of a particular advertiser. It is one of the world's most common and massive cyber-world scams and one of the most difficult to combat. Kshetri (2010) argues that illegitimate clicks on PPC advertisements have rekindled debate about online advertising's effectiveness, as search engine network partners, competitors, and unhappy employees can all generate illegitimate clicks. Fraudulent clicks have plagued digital advertisement for many years already, with annual losses in billions. Though there are only estimations to the click frauds damages, most research and consulting firms estimate that 10 to 20 percent of ad clicks are fake.

Recent reports show that a $19 billion was lost globally in 2018 to click frauds and anticipates the loss to reach $44 billion by 2022 (BusinessWire, 2017). A study conducted by CHEQ, a renowned cybersecurity company, estimates that marketers have lost $23 billion in 2019 alone on ad frauds (CHEQ, 2019). Advertisers have been criticizing ad publishers (e-intermediaries) for not doing much to combat click frauds. In response to such criticism, some publishers use automated filters to overcome fraudulent clicks. Despite that, many still believe very little progress has been made (Dinev et al., 2008). In a nutshell, not only do click frauds affect cost but also jeopardize ad campaigns and tarnish trust in this advertising model (Antoniadis et al., 2019). Blockchain could therefore be a solution to this severe problem.

Due to its immutability, transparency, and decentralization nature, blockchain is believed to mitigate click frauds. As blockchain offers traceability, tracking ad clicks becomes easy, and confirming their legitimacy is therefore possible. The giant car maker Toyota and the global ads agency Saatchi & Saatchi, for example, have partnered with the blockchain-based company Lucidity in a pilot project aimed to utilize the blockchain to verify the authenticity of ad clicks, eliminate wasted spending, and with this optimize the company's ad campaigns (Alexandre, 2018). Nancy Inouye, Media Director at Toyota Motor North America, says that the pilot project has, so far, powered a 21% boost for the company's ads (Barley, 2018). Using blockchain to trace ad clicks not only does it prevent fraud — and thus reduces cost — but also allows advertisers to better assess consumer's habits and thereby orchestrate targeted campaigns, optimize efficient budgets, and set accurate long-term strategies (Antoniadis et al., 2019). Ubex, Pinmo, and adChain (besides many others) are emerging blockchain start-ups that aim to tackle ad click frauds to enhance the performance of online advertisements.

Reinforcing trust and transparency

Because consumers' buying decisions are primarily based on what brands promise, consumers' trust is essential to a brand's success (Kim et al., 2008). In an online study conducted in 2019 by Edelman, the world's largest public relations and marketing consultancy firm, 67% agree that unless they trust the company, they will stop buying its product even if it has a good reputation (Edelman, 2019). The study also shows that 81% of the 16,000 surveyed respondents link their buying consideration to the level of trust. It also indicates that trusted brands are rewarded with long-lasting customer loyalty. Unfortunately, for brands, the study concludes that only 34% of consumers trust most brands, which consequently affects future buying decisions and diminishes the probability of long-term loyalty.

Furthermore, previous researches suggest that a critical prerequisite in trusting a company is the level of transparency it demonstrates (Kang & Hustvedt, 2014). Transparency implies openness, communication, and accountability; it means showing the whole truth about the information presented to consumers and the public and making it easy to see what and how actions are performed (Ball, 2009). Transparency also refers to the accessibility, usability, informativeness, understandability, and auditability of information (Fontana et al., 2018). In the past, companies' success depended on how much dressing they put on, whereas today, success depends on the extent they undress (Antoniadis et al., 2019). Big brands like Nike, Gap, Macy's, Microsoft, and so many more realized the importance of connecting closer with their customers by being transparent about their supply chain, labor issues, the provenance of their products, and so on (Kang & Hustvedt, 2014). Blockchain is therefore seen as a solution to reinforce transparency and build trust (Antoniadis et al., 2019; Ertemel, 2018).

By design, blockchain entails a trusted ecosystem. It removes ambiguity and uncertainties because transactions are embedded in immutable, timestamped, and transparent records (Ertemel, 2018). A consumer wishing to examine a brand's adherence to specific product quality criteria can do so with the traceability feature of blockchain. Therefore, brands can be held accountable should they, for example, purchase raw materials from untrusted sources or use under-age laborers from third-world countries to produce a product. The more transparency there is, the higher the probability brands will listen to consumers' concerns and meet their expectations. Label Insight, a company specializing in product data, surveyed 2,000 consumers in 2016 and concluded that 56 percent of those surveyed said they would be loyal to a company for life if it provided complete transparency. Additionally, 81 percent said they would be willing to sample a brand's entire range of products if they were comfortable with its degree of transparency (Kline, 2017). For today's business, transparency and trust are imperative for long-lasting loyalty, and blockchain is deemed capable of fostering a transparent and trustworthy environment.

Counterfeit products, in addition, cost brands annual losses in billions of dollars and jeopardize their reputation. Boston Consulting Group (BCG), a well-known consulting firm, reports, between $75 billion and $200 billion in counterfeit drugs are sold each year. In the electronics industry, fake parts cost component manufacturers about $100 billion annually. Moreover, about 10% of all items for sale are counterfeited in the European luxury goods market, representing approximately $28 billion in lost value (Bhatia et al., 2019). A report by the Organization for Economic Cooperation and Development and the European Union's Intellectual Property Office indicates that imported counterfeit goods reached $509 billion in 2016 alone (Venkataraman, 2019). Companies have suffered for too many years from counterfeit products, and consumers who look for authentic products face uncertainty when purchasing online. Big online retailers like Alibaba face major challenges and criticism as counterfeit products are sold on their platforms. The counterfeit products trade in Alibaba's Taobao is too high that the U.S. Trade Representative put the online company on the piracy blacklist (Reuters, 2018). Too many multinational corporations whose products are sold in this world's biggest e-commerce platform also expressed continuous frustration about the level of counterfeit products, and have long pressured Alibaba to safeguard the lost sales and endangered reputation of their brands from counterfeit products (Schuman, 2015). In response to this accumulated pressure, Alibaba — like many other companies — turned to blockchain. The company is currently running a blockchain pilot supported by IoT to track and authenticate two food products from Blackmores (Australia) and Anchor (New Zealand). Shoppers can simply use their smartphones to scan the product's tag to reveal its provenance. The company believes that once the pilot is complete and if successful, the framework could form the basis of a global supply chain model applied across all of Alibaba Group's ecommerce markets (Millward, 2018). Therefore, blockchain could be an innovative tool for companies to ascertain authentic products and thus increase their sales and safeguard their reputation.

Enhancing privacy protection

It is hard to imagine living in a world without the internet. It helped us advance in every imaginable area and made the world seem tiny. The internet is the social media that connects people, the global shopping mall for consumers, the wealth of information for scientists, researchers, and academics, and the globalization bridge to every country, town, and village for businessmen and economists (Ravasan et al., 2014). However, one thing that the internet has backfired on us is the level of unprecedented personal data exposure and privacy intrusiveness.

For as long as e-commerce and social media have existed, a wealth of personal data stream daily, with increasing concerns of misuse and abuse. Trading consumer personal and behavioral data has become a regular business for many companies. The so-called data brokers collect and sell the data to ad agencies who swarm consumers with advertisements.

As of May 2020, there exist approximately 4000 data brokers worldwide (WebFX, 2020), some of which are enormous! Singer (2012) studied one of the largest data brokering companies in the world, Acxiom. The company uses 23,000 servers to collect and sell the personal information and shopping preferences of around 500 million consumers to the highest bidder. She says, Acxiom knows where you live. It knows what you do. It peers deeper into American life than the I.R.S. or those prying digital eyes at Facebook and Google. If you are an American adult, the odds are that it knows things like your age, race, sex, weight, height, marital status, education level, politics, buying habits, household health worries, vacation dreams — and on and on. Furthermore, one can't help noticing (after shopping or just searching for a particular commodity) the popup ads that follow consumers from one website to another in a quite intrusive and annoying manner.

Privacy intrusiveness and data exposure have frustrated consumers for many years (Antoniadis et al., 2019). Surveys are conducted regularly to measure such concerns. A 2019 survey by the Pew Research Centre revealed that half of Americans have decided not to use a product or service because of privacy concerns and they were worried about how much personal information would be collected about the consumers (Perrin, 2020). Additionally, a survey by the research company Verve concluded that 60% of respondents (n = 2,400 UK consumers) said that they intentionally provide false information when submitting their data online because of privacy concerns (WARC, 2015). Such misleading information is therefore detrimental to effective marketing campaigns. To mitigate these privacy issues, blockchain could be a viable solution.

Due to its pseudonymization feature, blockchain entails a privacy-by-design ecosystem (Antoniadis et al., 2019).   It is impossible to see the actual identity of the users. This gives consumers total control over their credentials, which they are the only ones to decide how much data and with whom to share (van Rijmenam, 2019). In such a case, data protection is at its highest level, in a new consumer-centric environment in which: a) confidence in the system is restored; b) data cannot be commoditized by third-parties; c) brands can motivate their targeted consumers to share their data for rewards (Zyskind & Nathan, 2015),   and, in return, consumers present accurate information and interact with advertisements.

The aforementioned ecosystem would encourage consumers to engage more with brands and provide accurate information for better analytics, which would allow marketers to devise effective campaigns with optimized budgets. Enough evidence, dubbed as 'The Paradox of Personalization", shows that consumers are annoyed for being followed with "tailored" ads after shopping or enrolling in loyalty programs. Hence, engagement with brands and their loyalty programs are minimal due to this privacy concern (KPMG, 2019). Furthermore, Edelman's study also found that 3 out of 4 consumers try to avoid ads. Therefore, it is logical to give consumers the power to choose what ads to view since they ultimately digest them. Incentivizing consumers to view brands' ads, therefore, would be beneficial for both parties. For brands, it means saving money because their ads are viewed only by interested consumers

instead of "throwing ads to the wall and seeing what sticks" current advertisement strategy. And for consumers, it develops a sense of loyalty and engagement with the brands, plus money!

Several blockchain start-ups have strived to present privacy-preserving applications. Wibson, for example, launched in 2017 a blockchain-based marketplace that uses smart contracts to facilitate the transaction of personal information between sellers (e.g., consumers) and buyers (e.g., ads agencies), and the payment is Wibson Tokens (WIB) (Futoransky et al., 2020). The company's co-founder and CEO Mat Travizano says, "Consumer data is now the world's most valuable asset. The Wibson platform and token provide consumers an easy way to profit from the personal data they create every day while asserting full rights of ownership over their personal information" (CISION, 2018). Chema Alonso, Chief Data Officer of Telefonica of Wibson, says, "Data is fueling growth for the biggest companies in the world, but new models like Wibson's are emerging to reshape the space. With all the developments around personal data, Wibson is building an impressive team that's focused on a future when consumers demand control of their data" (CISION, 2018). Other start-ups that utilize the blockchain to enable consumers to control and share their data for financial incentives include Blockstack and Oasis Labs, among many others.

Empowering digital marketing security

Data security is an immense problem for the entire world. A 2016 cybersecurity report by Cybersecurity Ventures, sponsored by Herjavec Group (a well-known Canadian IT company), predicted an increase of global annual loss to cybercrimes from $3 trillion in 2015 to $6 billion in 2021. In 2020, this prediction was reaffirmed on the company's website: "Cybercriminal activity is one of the biggest challenges that humanity will face in the next two decades" (Ventures, 2019). This cybercrimes problem represents the greatest transfer of economic wealth in history, risks the incentives for innovation and investment, and will be more profitable than the global trade of all major illegal drugs combined (Morgan, 2018).

Cybercrimes are so ubiquitous that they impact almost every industry, including e-commerce (Huntsman, 2019). Many studies suggest that online cybercrimes (e.g., theft of consumers' personal information, credit cards, and bank accounts) have diminished consumers' confidence and, consequently, impeded their online engagement. A Forbes article by Steve Olenski (2016) argues that the custom of earning the trust of customers and building a foundation of loyal buyers is at the heart of every online company. Nevertheless, marketing endeavors can be swiftly untangled by the increasing threat of cybercriminals. Companies realize the long-term implications of cybercrimes to their online business and have always adopted measures to eliminate or significantly reduce such threats (Smith, 2004). Nonetheless, cybersecurity continues to be a major concern and a top priority for digital marketing as cybercrimes are still on the rise (Boone, 2017). Marketing and IT experts believe

blockchain could be the solution to this long-standing problem (Antoniadis et al., 2019; Ertemel, 2018).

The foundation of any security system is the Information Security Triad: Confidentiality, Integrity, and Availability (or CIA). The essence of confidentiality is restricting data access to those allowed to see it; integrity, furthermore, refers to the assurance that the data represents the truth and that no alteration (intentional or nonintentional) to its content has occurred; and availability means that data is accessible to authorized users in an appropriate timeframe. Blockchain enforces the CIA model in the following way. It applies asymmetric encryption, which leads to data confidentiality, especially in private blockchains. The rigorous consensus process and immutability characteristic of blockchain guarantee data integrity. Any attempt to tamper with consumers' data or steal their credentials is almost impossible, especially in public blockchains. Finally, since blockchain is decentralized and distributed, it is always available. Since blocks are sequential and timestamped, one can conveniently trace the history of transactions and data; every time a new block is added to the chain, every participant in the network gets near real-time updates.

Enabling Creative Loyalty Programs

A loyalty program is a brand's promise to reward its customers for their purchases. The rewards come in different forms, such as points, instant discounts, and cashback. It is considered an important marketing tool to attract customers, reach their satisfaction, and presumably achieve their loyalty (Tahal, 2014). A good loyalty program stimulates continuous repurchase and margin growth, while a bad loyalty program has a reverse effect. A study showed that consumers who are satisfied with loyalty programs are almost 80 percent more likely to continue purchasing from the brand (Mindtree, 2020). Research by Technical Assistance Research Program (TARP) found that a primary reason for customers' dissatisfaction and leaving a brand is unattractive loyalty programs (Tahal, 2014). TARP also carried out another study in which it concluded that 37% of dissatisfied customers do not complain to the company for not delivering its promises. They just simply switch to another brand (Goodman & Newman, 2003). That leads to negative word-of-mouth in the market. A Harvard study revealed that negative word-of-mouth has market damage to the brand twice as much as positive word-of-mouth has a positive effect (Goodman & Newman, 2003). Customers who do complain and show frustration about loyalty programs often say that the companies do not keep their promises, the rewards are obtained with difficulties, promised rewards have little value, and privacy protection is minimal (Stauss et al., 2005). Millennials, furthermore, are believed to be the driving force to fundamental changes in loyalty programs. Accordingly to Klynveld Peat Marwick Goerdele (KPMG International), 96% of millennials say companies should find new innovative ways to reward customers, in an online survey of 18,520 respondents (40% millennials) from 20 countries (KPMG, 2019). Millennials are seen as having a sense of entitlement, but this is a misunderstanding. They like to use technology

to do things 'smart', which is now available, encouraging them to try new things. (KPMG, 2019). Therefore, blockchain could perhaps answer the sought change for more innovative, attractive, and effective loyalty programs.

Blockchain is envisaged to reform loyalty programs. Several blockchain start-ups offer loyalty program platforms that, allegedly, take loyalty programs to another height, two of which are: Pei and REM Loyalty (Mire, 2019). Pei has partnered with renowned brands (e.g., Papa John's, Taco Bell, Starbucks, Target, Uber, Nordstrom, H&M) to offer customers a new form of loyalty program that is easy, fast, and attractive: an instant cashback (in the form of bitcoin or US$) for every purchase. REM Loyalty platform—built on the Stellar Blockchain82— offers a 'lifestyle rewards program' in which participants have one single access point to loyalty programs from every hotel and airline in the world. It also partnered with big brands like Apple, Amazon, Uber, Caffe Nero, Virgin Atlantic, Hyatt, Tesco, and more. The rewards are in the form of REM tokens that do not expire. Users can also convert REM Token to fiat money. Other blockchain-based platforms that offer appealing loyalty programs include LoyalCoin, Sandblock, and GATCOIN, among many others.

Methodology

Data Collection

The data used for this research were collected in two methods: a) secondary data (e.g., articles written by marketing and blockchain experts in the academic field and published by credible journals; articles published by recognized institutions and magazines such as Harvard Business Review, McKinsey & Company, and Forbes; up-to-date articles from technology contributors, researchers, and scholars, published by various known websites, such as medium.com) and b) an empirical study, as primary data collection, in the form of an online survey. The survey contained a total of 18 close-ended questions that covered the six study areas (benefits). There were two types of questions with predefined answers that corresponded to predefined statements. At the end of each question, also, open space was given, so respondents had the opportunity to elaborate on their answers and express further opinions. The close-ended questions aimed to create enough quantitative evaluation and analysis for each question about each study area. Meanwhile, giving respondents the chance to elaborate in detail was considered an essential part of the questionnaire because it contributed towards improving the interpretation of the overall results and provided further valuable qualitative material. The survey was distributed online in Google Forms in March-May 2020.

Survey Sample

This research carefully selected qualified marketing and blockchain experts from the academic arena (professors and doctorate students who had conducted some research about blockchain and published journal articles), as well as the private sector (blockchain

companies that developed blockchain applications for marketing areas such as loyalty programs and advertisements). The total number of invited experts to participate in the survey was 77, from which 22 responded. The response rate is therefore 29%. While half of the respondents had up to 2 years of marketing experience, 13.6% (3) had over 10 years of marketing experience and 31.8% (7) had 6 to 10 years of experience in marketing. Regarding the geographic locations of the respondents, 86.4% (19) came from the EU, 9.1% (2) from Asia, and 4.5% (1) from North America. Before contacting the experts, the researcher ran a pilot survey. Two Masaryk University PhD level marketing experts who had previously researched blockchain were invited to verify the logic behind each question and respond to the survey. Both respondents confirmed that the survey is in line with the thesis questions and objective.

Results

This research aims to validate the six benefits of blockchain-in-marketing through findings drawn from secondary data collection (the literature review) and primary data collection (the empirical study survey). From the findings and discussion of this research (explained in this section), we aim to gain a clearer vision of the future of blockchain applications in marketing.

Fostering disintermediation

From the survey participants, 36.3% (8) strongly agree, and 50% (11) agree that blockchain can foster disintermediation and restructure marketing and marketing concepts. By achieving that, 27.2% (6) strongly agree, and 54.5% (12) agree that a strong relationship between brands and consumers will forge; however, 13.6% (3) of respondents disagree with that. Furthermore, 36.3% (8) believe that such a new ecosystem will allow marketers to efficiently communicate their content to consumers and reduce the cost to a very high extent, and 31.8% (7) agree with that to a high extent. In contrast, 13.6% (3) see a medium impact to cost, and communication effectiveness should disintermediation ever happen, and 9% (2) don't see any impact at all. Also, a large portion of the surveyed experts—50% (11)—agree that consumer-brand direct interaction could encourage higher consumer engagement in campaigns with more authentic reviews; 36.3% (8) strongly agree with that.

The findings illustrate an overall agreement that blockchain does foster disintermediation indeed. However, two major issues need to be addressed: the identity of users and interoperability with other systems. The first issue relates to identity. Since a user's identity in a public blockchain is pseudonymous, no one in the blockchain network knows the other. While this is a suitable privacy protection mechanism, it is considered a drawback when a user's real identity is required. Many believe the middleman will always be needed to verify the "actual" user's identity to access certain files or use a specific service (Nathan, 2021). The need for real identity verification was one of the main reasons private blockchains came into existence so that enterprises can allow only certain users to log in to their blockchain network.

So, if a central authority is required to validate and control who joins the private blockchain network, then, by definition, this is not a decentralized network after all. Therefore, if all enterprises use private blockchains, it is hard to imagine data flow in a cloud of interconnected blockchain networks without censorship.

Consequently, the blockchain's disintermediation characteristic weakens or maybe vanishes. The second concern is interoperability. Currently, blockchain networks (public and private) are closed systems. Only those connected to a blockchain network can exploit its disintermediation advantage. The endeavors to interconnect blockchain networks with other systems are a long way to come. Unless blockchain finds its way to overcome the interoperability issue, marketers will have a limited audience. Besides, even if blockchain networks succeed in connecting with other non-blockchain networks that use intermediaries, blockchain users will still have to go through those intermediaries to access the other networks' content, violating the disintermediation principle of blockchain was fundamentally designed to foster. As it stands now, blockchain is merely a reef in a huge ocean. So, there is absolutely no pressure on non-blockchain systems to work hand-in-hand with the blockchain community to overcome the interoperability issue. Therefore, only when blockchain technology is adopted on a considerable scale within a vast ecosystem that connects many blockchain networks, fostering true disintermediation that presents tangible value to marketers and brands and consumers can then be foreseeable.

The findings also indicate that disintermediation assumes a strong brand-consumer relationship, with 27.2% (6) of the respondents strongly agreeing and 54.5% (12) agreeing to this statement. However, 13.6% (3) of respondents who disagree with this assumption indicate that fostering disintermediation does not necessarily lead to a strong relationship. Disintermediation is only a means of bringing stakeholders closer so that brands and marketers better understand consumers and their needs. Other factors such as the level of a brand's trustworthiness and transparency, the product's value (attractiveness, quality, and price), and the brand's loyalty programs are essential for consumers' engagement and long-term loyalty. Therefore, disintermediation becomes significant if in parallel with the aforementioned factors.

Combating click fraud

From the survey respondents, 54.5% (12) strongly agree that blockchain can combat click frauds to a very high extent, 18.1% (4) to a high extent, and 18.1% (4) to a medium extent. On the other hand, 9% (2) see negligible importance of blockchain for click frauds. Also, while 54.5% (12) of respondents strongly agree and 22.7% (5) agree that combating click frauds could contribute to a more trustworthy digital marketing environment, 13.6% (3) are not sure (neutral). Furthermore, 36.3% of respondents strongly agree that annihilating click frauds reduces ad costs, eliminates irrelevant ads, and helps to manage data clicks; 45.5% (10) agree with this claim, while 13.6% (3) are not too confident about it.

Even though the overall findings show a positive indication of blockchain's capability to combat ad click frauds, major issues must be considered. In public blockchains, for example, the number of transactions per second is quite limited. Also, transaction speed is slow because of the Proof-of-Work (PoW) consensus protocol that public blockchains use. On the other hand, private blockchains use a different consensus mechanism called selective endorsement, which allows for greater transaction volume at a faster speed (Bamakan et al., 2021). While this could alleviate the scalability and speed issue, the need for a robust network that accommodates massive data traffic is much greater than what private blockchains can deliver. Another crucial issue is, again, interoperability. The world consists of interconnected networks. If private blockchains are isolated from the rest of the world, it is impossible to see any major use for blockchain's traceability feature utilized beyond each network. Besides, we live in a world where digital advertisements are controlled by central systems. According to an article by Justin Musterman (2017) (a member of the Forbes Technology Council) and published by Forbes magazine, "over 60% of all digital advertising occurs on Facebook and Google". So, suppose blockchain's traceability feature was to be implemented for combating click frauds on an economic scale. In that case, scalability and speed issues must be resolved and one of these scenarios must occur: a) these gigantic networks (Google and Facebook) must be flexible—and willing—to consolidate their systems with other blockchain networks (which is hard to imagine now), or b) there must be a stand-alone network of interconnected private blockchains in which marketers and consumers can communicate independently from Google, Facebook and other legacy advertisement mediums. And this is foreseeable in the coming 5-10 years. Experts believe blockchain is capable of combating click fraud. While this could be theoretically true, the aforesaid issues would need to be addressed before marketers and consumers reap the benefit of this capability in practice.

Reinforcing trust and transparency

50% (11) of respondents strongly agree, and 40.9% (9) agree that blockchain is a 'trusted system by design'. Besides, 59% (13) believe that such a trusted ecosystem provides a transparent medium in and through which brands and consumers can communicate effectively and securely to a huge extent, and 31.8% (7) agree with that to a large extent. None of the survey respondents disagreed with the principle of blockchain's capability to reinforce trust and transparency. Furthermore, 27.3% (6) strongly agree, and 68.2% (15) agree that blockchain can eliminate the problem of counterfeit products that have adverse effects on a brand's reputation and financial losses. Only 4.5% (1) of respondents disagree that blockchain will combat counterfeit products.

From the three study areas that have been covered so far (fostering disintermediation, combating click frauds, and reinforcing trust and transparency), 'reinforcing trust and transparency' seems to receive the highest level of agreement with the survey respondents. While this gives us more confidence about blockchain in this specific study area, it is essential to evaluate whether "trust" and "transparency" really exist in blockchain, and where and how

exactly they fit in our thesis objective: validating the claim that blockchain is capable of "reinforcing trust and transparency". Blockchain's primary application was in cryptocurrencies. The use of sophisticated consensus algorithms allowed users who do not necessarily trust each other to securely exchange cryptocurrencies across borders without the need for a middleman. For that, it gained its reputation as a public ledger that created a 'trusted ecosystem'. Enterprises liked blockchain for its immutability characteristic and traceability feature as multiple industries crave for such a genius design. However, enterprises were not too fond of blockchain's total decentralization and transparency, and the idea of 'giving up full control' and 'exposing sensitive data in the open was (and still) incomprehensible. Therefore, private blockchains were developed to accommodate the need and criteria of enterprises. On the one hand, private blockchains are faster and more scalable than public blockchains because the number of participants is limited, and the consensus protocols are more efficient. On the other than, transactions in a private blockchain are validated by "trusted" nodes preselected by the central authority of the network that predefines participation rules and level of access to the network resources. Therefore, the trust issue in private blockchains depends on the participants in the network, not on the sophisticated algorithms that involve mass consensus as initially designed for public blockchains (e.g., Bitcoin). Hence, the 'trust by design' claim becomes a weak argument for private blockchains but a solid argument when it comes to cryptocurrency applications that run in a public blockchain. In a marketing context, therefore, companies that use private blockchains (or even public blockchains for the same matter) do not necessarily imply trustworthiness, not at all. They must show in actions that they're worthy of trust.

Furthermore, most companies nowadays use private blockchains that exploit the immutability and traceability features to, for example, track the origin of goods and thus combat counterfeit products. While this helps companies become transparent in front of their customers, there is a crucial challenge, scalability. Private blockchains perform well because they have fewer participants, so the load on the network is not near as heavy as public blockchains. However, once there is a need to increase the number of participants and transactions, problems await. For instance, let's take Alibaba's blockchain that traces two products from Australia and New Zealand as a pilot project. If the project succeeds for these two products and the company wishes to go big, Alibaba will have to account for millions of their customers and the thousands of products that would need to be in the blockchain. At the time being, it is highly doubtful such mass scalability is achievable. Therefore, blockchain developers need to solve the scalability issue to a vast extent before full-scale is achieved and consumers and companies reap the benefit of the transparency of products' provenance.

Enhancing privacy protection

The majority of the survey respondents agree that blockchain is capable of enhancing privacy protection; from the total participants, 18.1% (4) strongly agree, and 50% (11) agree. However, 27.3% (6) are not so sure (neutral), and 4.5% (1) disagree that blockchain will ever

enhance consumers' privacy protection. Meanwhile, half of the respondents strongly agree that blockchain is a privacy-by-design technology and thereby protecting consumers' data; 36.3% (8) agree with that, while 9% (2) disagree. When we talk about blockchain's ability to enhance privacy protection, it is crucial to pinpoint which blockchain are we referring to, public or private blockchain? To address this question, we compared (1) the two types against each other in terms of privacy protection in table 1, and (2) compared their compliance with major privacy protection regulations such as the European Union General Data Protection Regulation 2016/679 (GDPR) in table 2.

Table 1. Privacy protection comparison between public and private blockchains

Public Blockchains	Private Blockchains
The user's identity is a pseudonym.	The user's identity is not a pseudonym, but a 'real' user's identity is required to log into the network.
Block's data are stored indefinitely	Block's data are stored indefinitely but can be removed if the blockchain owner wants to.
Block's data are visible to everyone in the network	Block's data can be visible to everyone in the network or only to the intended user (s), as per the rules predefined by the network owner.

Table 2. Public and private blockchain's compliance with GDPR

Privacy Requirements by GDPR	Public Blockchains	Private Blockchains
Personal data is anonymous.	✓	X
Personal data is stored in the chain for as short a period aspossible, just for the period, the data is needed.	X	✓
Individuals have control over their data	X	X
Modification, correction, or erasure of data at any time at the individual's request is possible.	X	✓
There must be a legal basis for collecting and processing personal data, e.g., a) performing a contract, b) complying with a legal obligation, or c) the processing of data isnecessary by a third party, all of which would have a prior consent by the individual. Blockchain fulfills at least one of these requirements.	✓	✓
Maintaining proper security to prevent security breaches.	✓	✓
Data integrity – data is protected from unauthorized changesto ensure that it is reliable and correct	✓	✓
Data confidentiality – data is protected from unauthorizedviewing and other access.	X	✓
Restricting transfer of data across borders, especially incountries where GDPR is not followed.	X	✓

Although public blockchains seem to be less compliant with GDPR than private blockchains, companies in a public blockchain can't monetize consumers' personal information, while in private blockchains the network owner can do so. From a consumer's perspective, this is perhaps the most crucial part of their privacy protection, and this gives

public blockchain the upper hand in personal data protection. That been said, consumers may be more comfortable and confident dealing with public blockchains than private ones and thus would not need to provide false personal information. Additionally, while many blockchain startups provide consumers with the opportunity to monetize their data by sharing them with marketers, this idea already exists in traditional systems. The Solid project, for instance, uses Semantic Web technologies to do the same thing, enabling consumers to share their data with marketers for monetary gain. Therefore, it is essential to take a step back and ask basic questions: do consumers need their data to be protected to trade them with marketers for financial gain? If that is the primary purpose, there is no need for blockchain as other more accessible solutions are available. Otherwise, there is more to blockchain than just personal data exchange.

Empowering digital marketing security

Because of its immutability, blockchain gained a reputation of being hack-proof, which, as the findings from the survey confirm, empowers digital marketing security. While 50% (11) believe that blockchain empowers digital marketing security to a high extent, and 36.3% (8) affirm this to a very high extent, 9% (2) see a medium extent to such impact, and 4.5% (1) think blockchain does not empower digital marketing security. Also, 45.4% (10) strongly agree, and 36.3% (8) agree that by using blockchain, brands are protected, and consumers have a single version of the truth about a brand's values and characteristics; on the other hand, 9% (2) are neutral, and 9% (2) completely disagree with such statement.

Through complex consensus algorithms used by public blockchains, data cannot be tampered with. On top of that, decentralized and distributed prevent a single point of failure seen in centralized systems. Public blockchains can therefore empower digital marketing security and prevent cybercrimes. While this could be true for public blockchains, private ones may not qualify to the same level as public blockchains because of speculations about their decentralization issue. The unique identity of blockchain for being immutable, decentralized, and distributed entails a truthful and trusted system. While this has an excellent value for consumers to observe the truth about a brand's values and characteristics, it still depends on a brand's ethical values and its level of corporate social responsibility adherence. Blockchain is a technology that cannot replace ethics. Should brands present the truth about themselves, public blockchains can then preserve their integrity, not enforce it, and once that happens, consumers can be more confident about the whole system altogether.

Enabling loyalty programs

In general, the survey seems to confirm the claim in the literature that blockchain has the potential to improve how loyalty programs are designed, tracked, and communicated to consumers (and hence reducing complexities); 54.5% (12) strongly agree, and 31.8% (7) agree with this statement, while 9% (2) are not so sure, and 4.5% (1) disagree. Also, 63.6% (14) agree, and 31.8% (7) strongly agree that, as a single point of truth, blockchain presents an

opportunity to unify loyalty programs and eliminate the incompatibilities in existing ones, while 4.5% (1) disagree. Besides, the majority of respondents—54.4% (12)—agree that by using blockchain, marketers can assess consumers' interaction with loyalty programs in real-time and thereby formulate more efficient ones that encourage more engagement; 31.8% (7) strongly agree with this statement, while 9% (2) strongly disagree and 4.5% (1) disagree. Meanwhile, 72.7% (16) agree, and 27.3% (6) strongly agree that blockchain allows consumers to track their loyalty points without the need for the possession of physical coupons; not a single disagreement with that. In this discussion, there are four major issues to be taken into consideration.

First, by using blockchain-based loyalty program applications, consumers can accumulate points from all merchants and redeem them whenever and wherever they want as they are not confined and limited to redeem their points on the shop or store where points were initially collected from. While this single-point of access makes it easy and fast to claim rewards and—presumably—encourages more engagement, one may argue that if consumers do not redeem points in stores where points are generated, brands may no longer be motivated to pursue such loyalty programs. From a brand's perspective, an actual measurement of the rewarded points is not clear at all when using blockchain because consumers can then redeem the collected points elsewhere. Why would company X embrace a loyalty program where a consumer is free to redeem the same points with company Y!

Second, most existing blockchain-based loyalty program platforms are third-party enterprises that use public blockchains (like Bitcoin and Ethereum) that reward consumers with cryptocurrency. As an advantage, adopting public blockchains in loyalty programs maximizes the number of merchants and consumers that can easily and quickly join the platform interact safely (as there are traditionally many fraudulent loyalty programs) and efficiently. However, two points need to be addressed: a) scalability and speed: loyalty programs aim to attract and retain as many customers as possible. With blockchain's scalability limitation, increasing consumers' engagement in such programs can potentially slow the network. Also, redeeming points in a blockchain may take time and cost money. Pei, for example, processes customers' requests to redeem their rewards in batches to avoid large mining costs associated with every transaction on the Bitcoin network. Besides, when a customer is rewarded with Bitcoin, conversion to fiat money will involve a conversion fee, and b) privacy: as data is permanent in a public blockchain, abiding by regulations like GDPR becomes an issue.

Third, some companies are launching their cryptocurrencies as rewards for engaging in their points-based loyalty programs, which means they have their own private blockchain solely for their customers. In this case, the scalability and speed issues are resolved — to a certain extent — but the privacy issue remains. Besides, suppose every company creates its own cryptocurrency (or coin). In that case, consumers will eventually end up with too many

types of coins, and that, maybe, becomes complicated and unmanageable because each has its fluctuating value.

Fourth, there already exist technologies for loyalty programs that serve the same purpose as a blockchain – single-point of access to collecting points from hundreds of merchants in various industries and redeeming them anywhere (e.g. Qantas). Some giant banks like American Express and Citibank also use 'cashback rewarding programs' that allow members to " … earn on ANY airline, ANY hotel, and ANY retailer — and letting them pool all of their points and redeem them for what they want when they want." (Feldman, 2018). The cool part is that blockchain-based loyalty programs reward cryptocurrencies. Also, transactions are immutable and transparent. Therefore, businesses need to evaluate the cost-benefit of choosing blockchain-based applications over existing legacy technology. On the one hand, using blockchain to reward consumers in cryptocurrency could be an attractive and trendy marketing tool to encourage more consumers' engagement. It can also help consumers manage their collected points from all merchants in a single and simplified spot. Besides, it can aid marketers in better understanding consumers' preferences. However, scalability, speed, and privacy remain enormous obstacles. Not to mention the very idea of companies giving points where they are redeemed with other companies who could be competitors.

Discussion

The results from the findings and discussion in the six areas demonstrate a general agreement that blockchain is indeed envisaged to impact marketing by providing a unique ecosystem through which these six benefits can be realized. However, the research concludes that determining the extent (value) of the impact depends significantly on the type of blockchain been used (public or private) and the ability to overcome the challenges and pending issues facing each type for every study area, as illustrated in the following table 3.

Table 3. Challenges and pending issues facing blockchain for each study area (benefit)

Study area (benefit)	Public (permissionless) blockchain	Private (permissioned) blockchain
Fostering disintermediation	- Pseudonymization is viewed as a drawback when 'real' identity is required.	- As a closed system subject to central authority control, the number of consumers is limited. - Interoperability.
Combating clickfraud	- Scalability and speed.	- Interoperability.
Reinforcing trustand transparency	- Total transparency presents a challenge to data confidentiality.	- Marketers and consumers are constrained to the level of transparency provided by the central authority that controls the network.
Enhancing privacy protection	- Low compliance with GDPR	- Medium compliance with GDPR
Empowering digital marketing security	- Lack of data confidentiality violates data security principles.	- Immutability is threatened, which leads to data integrity violations.
Enabling loyalty programs	- Scalability and speed. - Privacy issues, as consumers cannot withdraw their data from the blocks.	- Scalability and speed become an issue with more consumers wishing to participate in the programs. - Privacy issues, as consumers' data is prone to monetization.

Based on the results, we can conclude that marketers and brands cannot have a comprehensive blockchain that provides the six benefits in one package, at least not at the present time. For example, if marketers and brands wish to protect consumers' data, public blockchains could be a good choice. However, they must realize that the confidentiality of information is put in jeopardy. If, however, information confidentiality is more important than consumer data privacy, then private blockchains are a good option. Similar trade-offs must be put into consideration when trying to realize any of the other six benefits. Therefore, selecting the type of blockchain for marketing purposes depends entirely on which benefits marketers and brands wish to achieve from a business perspective. A few years down the road will reveal which type of blockchain would be the best fit for marketing applications, and that depends on how much and how fast the challenges and pending issues facing each type will be resolved.

Conclusion

The creation and increasing adoption of cryptocurrencies paved the way for several industries to exploit the many benefits of blockchain. The marketing industry, however, seems to be watching bashfully. If this attitude changes, we may observe a shift to an entirely new marketing ecosystem where more innovative marketing ideas and concepts are born. We believe that it is imperative to define a realistic scope of blockchain's business value to obtain more credibility when considering this technology for any application. From this research's observations and readings, blockchain seems to receive too much hype still. We have examined the technology's capabilities to solve several crucial issues for marketing; however, most of these solutions are still conceptual. Even if some are practically used now (e.g. tokens for loyalty programs), they still need some time to mature and streamline. After all, this is a young technology with ongoing experimentations that may, or may not, succeed. Nevertheless, if they do succeed, blockchain will indeed mark a new paradigm in our continuous digital evolution.

This research suffers from some limitations. First, the scarcity of literature about the impact of blockchain on marketing presented a challenge and limitation for the researcher to compare the findings and analysis stipulated in the discussion section against previous research. Second, although the online survey was a great tool that allowed the researcher to gather responses and opinions from selective experts, some limitations need to be considered. The response rate was not very high (29%). Considering the magnitude and future importance of the research, this might not be the ideal size of participation wished for.

For the marketing industry not to be left behind, a proactive approach is recommended. Rather than just waiting and watching other industries aggressively research and invest in this emerging technology and therefore become first to reap its benefits, the marketing community should exert more efforts in two major areas: a) conducting more researches and large-scale

surveys by major consulting companies and educational institutions; b) ramping-up collective investments among major enterprises to combat the challenges and pending issues and to carry-on various blockchain experiments tailored for marketing applications.

Conflict of interest

The authors declare no potential conflict of interest regarding the publication of this work. In addition, the ethical issues including plagiarism, informed consent, misconduct, data fabrication and, or falsification, double publication and, or submission, and redundancy have been completely witnessed by the authors.

Funding

The author(s) received no financial support for the research, authorship, and/or publication of this article

References

Alexandre, A. (2018). *Toyota Uses Blockchain Tech to Reduce Fraud in Digital Advertising Campaigns*.

Antoniadis, I., Kontsas, S., & Spinthiropoulos, K. (2019). Blockchain applications in marketing. *The Proceedings of 7th ICCMI*.

Ball, C. (2009). What is transparency? *Public Integrity*, *11*(4), 293–308.

Bamakan, S. M. H., Faregh, N., & ZareRavasan, A. (2021). Di-ANFIS: an integrated blockchain–IoT– big data-enabled framework for evaluating service supply chain performance. *Journal of Computational Design and Engineering*, *8*(2), 676–690.

Barley, M. (2018). Lucidity blockchain powers 21% boost for Toyota ads. *Ledger Insights*.

Bhatia, A., Yusuf, Z., Gill, U., Shepherd, N., Kranz, M., & Nannra, A. (2019). *Stamping Out Counterfeit Goods with Blockchain and IoT*. https://www.bcg.com/publications/2019/stamping-out-counterfeit-goods-blockchain-internet-of-things-iot

Boone, A. (2017). Cyber-security must be a C-suite priority. *Computer Fraud & Security*, *2017*(2), 13–15.

BusinessWire. (2017). *Juniper Research: Ad Fraud to Cost Advertisers $19 billion in 2018, Representing 9% of Total Digital Advertising Spend*. https://www.businesswire.com/news/home/20170926005177/en/Juniper-Research-Ad-Fraud-Cost-Advertisers-19

Casey, M. J., & Vigna, P. (2018). In blockchain we trust. *MIT Technology Review*, *121*(3), 10–16.

CHEQ. (2019). *CHEQ Report: Online Ad Fraud To Cost $23 Billion Globally in 2019*. https://www.prnewswire.com/news-releases/cheq-report-online-ad-fraud-to-cost-23-billion-globally-in-2019-300860628.html

CISION. (2018). *Wibson Launches Blockchain-Based Marketplace for Consumers to Profit from Their Personal Data*. https://www.prnewswire.com/news-releases/wibson-launches-blockchain-based-marketplace-for-consumers-to-profit-from-their-personal-data-300728956.html

Dinev, T., Hu, Q., & Yayla, A. (2008). Is there an on-line advertisers' dilemma? A study of click fraud in the pay-per-click model. *International Journal of Electronic Commerce*, *13*(2), 29–60.

Edelman, R. (2019). *Edelman Trust Barometer Special Report: In Brands We Trust*.

Ertemel, A. V. (2018). Implications of blockchain technology on marketing. *Journal of International Trade, Logistics and Law*, *4*(2), 35–44.

Feldman, D. (2018). *Blockchain & Loyalty: A Solution in search of a Problem*. https://medium.com/@dfcatch/blockchain-loyalty-a-solution-in-search-of-a-problem-6ba51218b5a6

Fontana, P., Diirr, B., & Cappelli, C. (2018). Transparency Challenges in Blockchain. *EGOV-CeDEM-EPart 2018*, 193.

Futoransky, A., Sarraute, C., Fernandez, D., Travizano, M., & Waissbein, A. (2020). Fair and Decentralized Exchange of Digital Goods. *ArXiv Preprint ArXiv:2002.09689*.

Goodman, J., & Newman, S. (2003). Understand customer behavior and complaints. *Quality Progress*, *36*(1), 51–55.

Harvey, C. R., Moorman, C., & Toledo, M. (2018). How blockchain will change marketing as we know it. *Available at SSRN 3257511*.

Huntsman. (2019). *Cyber crime affects every sector*. https://www.huntsmansecurity.com/blog/cyber-criminals-target-all-sectors/

Jallat, F., & Capek, M. J. (2001). Disintermediation in question: New economy, new networks, new middlemen. *Business Horizons*, *44*(2), 55–60.

Kang, J., & Hustvedt, G. (2014). Building trust between consumers and corporations: The role of consumer perceptions of transparency and social responsibility. *Journal of Business Ethics*, *125*(2), 253–265.

Khan, H., & Kushwah, K. K. (2021). Blockchain and the Future of Digital Marketing. In *Blockchain Technology and Applications for Digital Marketing* (pp. 250–275). IGI Global.

Kim, D. J., Ferrin, D. L., & Rao, H. R. (2008). A trust-based consumer decision-making model in electronic commerce: The role of trust, perceived risk, and their antecedents. *Decision Support Systems*, *44*(2), 544–564.

Kirkland, R., & Tapscott, D. (2017). *Getting serious about blockchain*.

Kline, K. (2017). Here's How Important Brand Transparency is for Your Business. *Inc. September*, *5*, 2017.

KPMG. (2019). *The truth about customer loyalty*. https://home.kpmg/xx/en/home/insights/2019/11/customer-loyalty-survey.html

Kshetri, N. (2010). The economics of click fraud. *IEEE Security & Privacy*, *8*(3), 45–53.

McGhin, T., Choo, K.-K. R., Liu, C. Z., & He, D. (2019). Blockchain in healthcare applications: Research challenges and opportunities. *Journal of Network and Computer Applications*, *135*, 62–75.

Millward, S. (2018). *Alibaba rolls out blockchain pilot to tackle fake food products*. https://www.techinasia.com/alibaba-fake-food-blockchain-pilot

Min, H. (2019). Blockchain technology for enhancing supply chain resilience. *Business Horizons*, *62*(1), 35–45. https://doi.org/10.1016/j.bushor.2018.08.012

Mindtree. (2020). *Case Study: How Mindtree revolutionized loyalty platforms and merchant onboarding with Hyperledger Fabric*. https://www.hyperledger.org/wp-content/uploads/2020/06/Hyperledger_CaseStudy_Mindtree_Printable.pdf

Mire, S. (2019). *Blockchain In Marketing: 23 Startups To Watch In 2019*. https://www.disruptordaily.com/blockchain-startups-marketing/

Morgan, S. (2018). Global cybercrime damages predicted to reach $6 trillion annually by 2021. *CyberCrime Magazine*.

Musterman, J. (2017). *No, Blockchain Won't Solve Ad Fraud*. https://www.forbes.com/sites/forbestechcouncil/2017/11/22/no-blockchain-wont-solve-ad-fraud/?sh=6a7260ce34e2

Nakamoto, S. (2008). *Bitcoin: A Peer-to-Peer Electronic Cash System. 2008*, 9.

Nathan, R. (2021). *Blockchain Won't Cut Out Intermediaries After All*. https://www.investopedia.com/tech/blockchain-wont-cut-out-intermediaries-after-all/

Perrin, A. (2020). *Half of Americans have decided not to use a product or service because of privacy concerns*. https://www.pewresearch.org/fact-tank/2020/04/14/half-of-americans-have-decided-not-to-use-a-product-or-service-because-of-privacy-concerns/

Ravasan, A. Z., Rouhani, S., & Asgary, S. (2014). A review for the online social networks literature (2005-2011). *European Journal of Business and Management*, 6(4), 22–37.

Reuters. (2018). *U.S. Puts Alibaba's Taobao on Blacklist for Counterfeit Products—Again*. https://fortune.com/2018/01/12/alibaba-taobao-blacklist-counterfeit-products

Rosenbloom, B. (2007). The wholesaler's role in the marketing channel: Disintermediation vs. Reintermediation. *International Review of Retail, Distribution and Consumer Research*, *17*(4), 327–339.

Saberi, S., Kouhizadeh, M., Sarkis, J., & Shen, L. (2019). Blockchain technology and its relationships to sustainable supply chain management. *International Journal of Production Research*, *57*(7), 2117–2135. https://doi.org/10.1080/00207543.2018.1533261

Schuman, M. (2015). Why Alibaba's massive counterfeit problem will never be solved. *Forbes, Nov*, 23.

Singer, N. (2012). *Mapping, and Sharing, the Consumer Genome*. https://www.nytimes.com/2012/06/17/technology/acxiom-the-quiet-giant-of-consumer-database-marketing.html

Smith, A. D. (2004). Cybercriminal impacts on online business and consumer confidence. *Online Information Review*.

Stauss, B., Schmidt, M., & Schoeler, A. (2005). Customer frustration in loyalty programs. *International Journal of Service Industry Management*.

Steve Olenski. (2016). *The Effect Of Cyber Crime On Online Shopping*. https://www.forbes.com/sites/steveolenski/2016/08/03/the-effect-of-cyber-crime-on-online-shopping/?sh=2f40d9e2b873

Swan, M. (2015). *Blockchain: Blueprint for a new economy*. O'Reilly Media, Inc.

Tahal, R. (2014). Loyalty programs in e-commerce and their perception by the young adult internet population. *Central European Business Review*, *3*(2), 7–13.

Tapscott, D., & Tapscott, A. (2016). *Blockchain revolution: How the technology behind bitcoin is changing money, business, and the world*. Penguin.

van Rijmenam, M. (2019). *How Blockchain Will Give Consumers Ownership of their Data*. https://markvanrijmenam.medium.com/how-blockchain-will-give-consumers-ownership-of-their-data-3e90020107e6

Venkataraman, M. (2019). *How Blockchain Can Fight Counterfeiting and Fraud*. https://www.globaltrademag.com/how-blockchain-can-fight-counterfeiting-and-fraud/

Ventures, C. (2019). *2019 official annual cybercrime report*.

WARC. (2015). *"Dirty data" threat to marketers*. https://www.warc.com/newsandopinion/news/dirty-data-threat-to-marketers/en-gb/35059

WebFX. (2020). *What Are Data Brokers – And What Is Your Data Worth?* https://www.webfx.com/blog/internet/what-are-data-brokers-and-what-is-your-data-worth-infographic/

ZareRavasan, A., Krčál, M., & Ashrafi, A. (2021). *Blockchain and Digital Transformation of Insurance Business Models   Order a copy of this article*. https://doi.org/10.1504/IJBC.2021.10041701

Zyskind, G., & Nathan, O. (2015). *Decentralizing privacy: Using blockchain to protect personal data*. 180–184.

Bibliographic information of this paper for citing:

Al-Ahwal, Taher M.; Mladenović, Dušan & ZareRavasan, Ahad (2022). Blockchain Implications for Marketing; A Review and an Empirical Analysis. *Journal of Information Technology Management,* Special Issue, 83-106. https://doi.org/ 10.22059/jitm.2022.87843