IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received July 13, 2018, accepted September 3, 2018, date of publication October 1, 2018, date of current version October 19, 2018.

Digital Object Identifier 10.1109/ACCESS.2018.2872694

Is Blockchain Ready to Revolutionize Online Advertising?

MATTI PÄRSSINEN[1], MIKKO KOTILA[2], RUBÉN CUEVAS RUMIN[3], AMIT PHANSALKAR[2], AND JUKKA MANNER[1]

[1]Department of Communications and Networks, Aalto University, 02150 Espoo, Finland
[2]BOTLab, Boston, MA 02215, USA
[3]Avenida de la Universidad, Universidad Carlos III de Madrid, 28911 Leganés, Spain

Corresponding author: Matti Pärssinen (matti.a.parssinen@aalto.fi)

ABSTRACT The 200-billion-dollar per annum online advertising ecosystem has become infested with thousands of intermediaries exploiting user data and advertising budgets. All key stakeholders in the value-chain are infected: advertisers with fraud, publishers with their diminishing share of advertising budgets, and users with their right to privacy. Blockchain presents a possible solution to addressing the critical issues in the online advertising supply chain. The question remains whether blockchain scalability, energy-efficiency, and token volatility issues can be solved in the coming years to the extent that online advertising could widely leverage trustlessness and the benefits gained from blockchain technology. This paper aims to review the current progress and to open a discussion to address the issues. We present new requirements for blockchain-based online advertising solutions. We have also analyzed the available solutions against the requirements and recommend directions for future research and solution development. Evidence from our research points out that blockchain is not yet ready to be widely implemented in online advertising. More research is needed, and new proof-of-concepts need to be developed before blockchain technology can be considered a trusted alternative for the current online advertising marketplace based on open real-time bidding.

INDEX TERMS Blockchain, online advertising, adtech, energy efficiency, transparency, ad fraud.

I. INTRODUCTION

Online advertising is a vital stakeholder of the Internet's economy. According to a 2015 IHS technology report, in Europe, 50% of online video revenue is generated through advertisements. With online editorial content, advertising generates 75% of the total revenue [1]. In the mobile application market, the share of ad-funded free apps is increasing compared to ad-free paid apps. Online advertising revenue has registered double-digit growth over the past decade – in the US in 2016, $72.5 billion in revenue was generated [2].

A growing trend in online advertising in recent years has been the move towards programmatic media trading. Programmatic advertising is designed for small advertisers and publishers to ease access to the online advertising market. The programmatic model enables dynamic advertising budget allocation with the desired context of publishers and the targeting of specific audiences efficiently [3] and at scale.

In the programmatic model, advertisers use trading desks to connect to demand-side platforms. Demand-side platforms connect trading desks with ad networks and exchanges. Publishers make their inventory available through exchanges, ad networks, or directly through trading desks [4]. Programmatic advertising has the disadvantage of being opaque and exposed to threats such as fraudulent activity. Programs can easily exploit the common event-based pricing model. The detection of fraudulent activities is a challenging task due to the large volume of transactions [3].

The capacity to connect hundreds of thousands of publishers with a similar order of advertisers in an automated manner, together with the promise of accurately targeted advertising, has caused digital marketing to rapidly evolve into a complex ecosystem where different intermediaries are focused on optimizing particular functions. This ecosystem operates effectively as a black box for the three key players: advertisers, publishers and users.

The online advertising ecosystem has become infested with thousands of intermediaries, whose business models range from exploiting user data to verification companies promising to help advertisers secure their advertising budgets. The principal parties in online advertising – users, advertisers and

publishers – have recently all pointed out concerns related to these intermediaries, the actual value they provide, and how in many cases they operate against the interests of at least one of the above-mentioned key players. Advertisers are concerned about fraud [5] and ad misplacement, publishers about their diminishing share of advertising budgets [6], and users about their right to privacy [7]. So far, the self-regulation efforts of the online advertising industry have not succeeded in mitigating fraudulent activities.

We claim that blockchain can be a practical solution to addressing issues burdening online advertising. An increasing amount of companies and experts in the online advertising industry agree with us [8]–[10] on this proposition. At the same time, we disagree with those claiming that blockchain technology is ready to be applied to solving online advertising problems. In this paper, we present a list of requirements to consider for blockchain to become a functional solution for online advertising. While some form of blockchain-based approach may indeed prove to be suitable for addressing transparency and authenticity issues eroding trust in online advertising, multiple essential questions require answers prior to achieving a possible industry-wide implementation. For example, whereas Bitcoin, the best-known implementation of blockchain technology, handles 500k transactions per day, the programmatic advertising ecosystem manages billions of transactions per day [11]. Scale, therefore, presents an open challenge.

Other concerns regarding the utilization of blockchain technology in online advertising include energy consumption and the rapid growth of the global carbon dioxide equivalent (CO_2e) footprint of the Internet. Current popular blockchain-based solutions offer poor energy efficiency when applied at a much lower scale than what online advertising would require.

This paper aims to review blockchain technology, present the requirements for blockchain adaptation in online advertising, analyze the current blockchain-based solutions available for online advertising, and evaluate blockchain platforms against the requirements above.

A scalable and energy-efficient blockchain paradigm, where trading tokens, at least initially, are pegged to currency, needs to meet the specific requirements of online advertising. In this regard, we will make the following contributions: a thorough review of the blockchain technology and its fundamental principles, requirements for utilizing blockchain as a solution in the online advertising industry, an analysis of the currently available blockchain-based solutions addressing online advertising, and blockchain platforms in respect to the requirements. These contributions create a solid base for further discussion on the broader adoption of blockchain for online advertising, particularly concerning addressing the scalability, energy-efficiency and token volatility questions.

Our final contribution is the conclusion of our study: to create a solution for overcoming the issues in online advertising, we identified six requirements that a possible solution must fulfill. These requirements are scalability, quasi-transparency, inability to modify blocks, non-repudiability, quality information and energy efficiency. We find that none of the reviewed blockchain-based online advertising solutions have the market adoption to suggest significant buyer confidence. We provide novel recommendations for solution developers on how to proceed in fulfilling the requirements.

The remainder of this paper is structured as follows: Section 2 presents the used materials and methods. Section 3 introduces the blockchain technology. Section 4 presents the requirements for online advertising implementations, and Section 5 analyzes the currently available blockchain-based solutions. The results are presented in Section 6 and discussed in Section 7, and finally, the conclusions are presented in Section 8.

II. MATERIALS AND METHODS

This paper is a review article. The aim is to present the current state of knowledge on blockchain technology and its possibilities in online advertising. We first review relevant articles previously published on blockchain, and secondly analyze the blockchain-based publicly available solutions to online advertising.

The blockchain technology review has been gathered from published articles and industry white papers. Blockchain is a somewhat new technology, and academic publications have not adequately addressed vertical solutions outside of cryptocurrency. In particular, there are no academic publications for online advertising, to the best of the authors' knowledge. Online advertising's specific requirements have been formed from industry sources, and the researchers' extensive knowledge of the industry and its primary challenges and constraints.

The analysis of currently available blockchain-based industry solutions and blockchain platforms are mainly based on publicly available sources. We have analyzed the solutions against the known specific requirements of online advertising. The gaps between existing solutions and online advertising requirements that need researchers' attention are based on the reasoning of the researchers and are open to falsification and future discussion. In Section 7, we suggest possible development and research topics regarding each of the presented requirements in Section 4.

III. BLOCKCHAIN TECHNOLOGY

The world is undergoing rapid change. This change is accelerated by the development of Internet technologies and the exponential growth of data. Blockchain could be the fifth disruptive technology after mainframes, PCs, the Internet, mobile communication and social media [12]. A blockchain is a distributed peer-to-peer database, which provides a technology for the decentralization of systems. Blockchain alone does not guarantee decentralization, but it does guarantee the distribution of data storage and transactions. The decentralized model has the potential for increased equality in storage, and the availability of information and resources.

Blockchain technology implementation alone is not synonymous with decentralization.

Blockchain can be utilized to facilitate transactions between nodes in a peer-to-peer network. What is transacted could be virtually anything: currency, votes, health data, ideas, predictions, storage capacity, computing power, or food, to name a few examples. So far, the emphasis has been on cryptocurrencies such as Bitcoin, and there has been less talk about the underlying innovation – the blockchain technology. We have noted the Initial Coin Offering (ICO) ecosystem, powered by another popular cryptocurrency, Ethereum, is rapidly shifting the focus, and new applications are introduced every week. Even though blockchain technology promises to transform human society in various ways, much work remains to be done before that promise translates into wide-reaching benefits for the average person. Today, the best-known successful new business models made possible by cryptocurrencies are malicious. Examples include ransomware attacks [13] and dark web markets [14] selling weapons, wholesale heroin [15], personal data, and murder-for-hire [16]. There are however many proven benefits from blockchain adoption, as is the case with Bitcoin being used to reduce e-commerce fraud [17].

A. DECENTRALIZED ARCHITECTURE

There is a well-established taxonomy [12], [18] for decentralized architectural objects. The first one is decentralized applications (DAPPs). A DAPP utilizes a network in a distributed fashion. Member information is secure and pseudonymously protected. The execution of operations is decentralized between member nodes. A blockchain-based DAPP must be an open source application operating autonomously without the possibility for a single stakeholder to control the majority of tokens. In addition, data and records must be cryptographically stored in a public blockchain. In DAPP, tokens must be generated with a standard algorithm and some or all of its tokens must be distributed at the birth of its operation. The protocol and the application must be further developed according to proposed improvements and feedback based on a majority consensus decision on these changes [12].

The second architectural object is decentralized autonomous organizations (DAO). DAO originates from artificial intelligence. It is a decentralized network of autonomous agents performing tasks without any human involvement. A set of rules controls DAO. Smart contracts act as agents, running on blockchains, which execute a range of predefined or pre-approved tasks. Execution is founded on events and changing conditions [12], [18].

The third architectural object is decentralized autonomous societies (DAS). DAS can consist of many smart contracts, or multiple DAPPs and DAOs operating autonomously. Examples of DAS include automatic markets and trading networks. DAS automatically transact unitized, packetized, and quantized resources. It is based on dynamically evolving conditions, user profiles, authorization, and bidding capabilities. DAS technology is used in smart energy grids, and it can have automatic bidding functions on the supply and demand side of operations. All stakeholders have automatic clearing mechanisms. The online advertising market can be considered a DAS [12], [18].

B. BLOCKCHAIN TECHNOLOGY OVERVIEW

Blockchain technology includes three essential components: the application, the protocol, and the cryptographic solution. The fundamental principle of a blockchain is presented in Figure 1. A blockchain consists of blocks, hashes, and hash functions. In Figure 1, the n-1 block in the middle records its hash into the block. Also, the hash of the n-2 is also recorded to the same block. The addition of the previous block hash cryptographically chains the current block to the previous block, forming a chain of blocks. A hash function is a mathematical algorithm that transforms input into an output. A cryptographic hash function is complicated to revert. This feature of a blockchain is called collision resistance [19]. Every block includes the timestamp of its creation and additional information based on the configuration of the blockchain in question. All blocks have the payload of their block and all the previous blocks' payload.

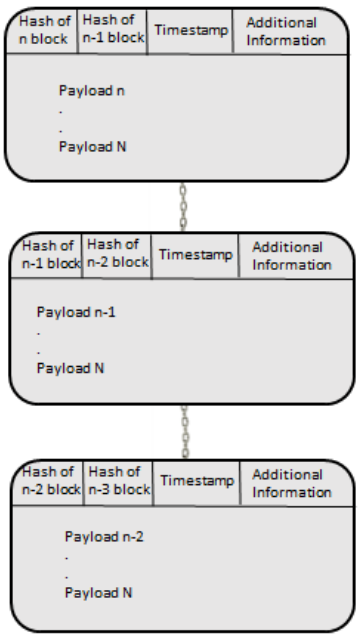

FIGURE 1. The fundamental principle of a blockchain, adapted from [20].

The functionality of a blockchain can be described in the following way: the node sending new data records the data into a block and then sends a broadcast about the new available block to the blockchain network. The nodes receiving the new block verify the block from the hash. If the payload was correct, it is added to a block. Proof-of-work (PoW) or proof-of-stake (PoS) algorithms are executed to the block by all member nodes. The new block is added to the blockchain once a consensus has been reached and all nodes verify this block [20].

One of the novelties of blockchain is the concept of ''the miner'' and how the miners unlock value in the blockchain – in the case of Bitcoin – by solving difficult computational problems. In blockchain storage, there is no double-send problem; each node is assigned with a private key and a public key. The fundamental functions of blockchain make it ''trustless'' in the sense that value can be exchanged with confidence without dependence on a trusted third party or central administration. Blockchain provides general architectural benefits like decentralized processing, redundancy, immutable public record, transparent access, and global reach [19].

There are three different kinds of blockchain: private, public, and hybrid [21]. In an entirely private blockchain, write permissions are monitored by a centralized decision making entity, and read permissions are either public or restricted. A private blockchain amounts to a permissioned ledger, whereby an organizational process of Know-Your-Business (KYB) and Know-Your-Customer (KYC) enables the whitelisting (or blacklisting) of a user identity. Public decentralized blockchains are accessible to every Internet user. All members can determine what blocks are added to the chain and what its current state is. Fully decentralized public blockchains need a consensus mechanism for the validating process.

The main difference between public and private blockchains is the level of decentralization, or how they ensure anonymity. There is a continuum between the two extremes, resulting in partially decentralized blockchains. Consortium blockchains constitute a hybrid between the public and the single highly trusted private blockchain. The continuum is also applicable to energy consumption; public blockchains, especially those using the trustless PoW consensus algorithm, consume vast amounts of energy compared to a trusted private blockchain.

The evolution of blockchain can be described by three significant releases [12] (we will refer to them as generations). The first-generation blockchains are currency-related, whereas the second-generation blockchains are smart contracts-related and the third concentrate on justice and other administrative applications. The second-generation blockchains provide solutions for the decentralization of markets and the means to transfer many other kinds of assets beyond currency. The smart contract-based second-generation blockchain is the main scope when analyzing the potential of blockchain technology in the context of online advertising. The third generation has the potential to circumvent the limitations of geographical jurisdictions and other vital functions of society such as voting, taxation, education, and healthcare.

C. THE CONCEPTS OF PROOF AND CONSENSUS

To provide the aforementioned authenticity and security properties, different implementations of blockchain protocols use different types of proofs. The most well-known proof is the one used in the context of Bitcoin, PoW. PoW was initially developed to defend against denial-of-service attacks and spam. The high total hash power of the blockchain network was needed to defend against a potential 51% of the network hash rate. Hashing could be performed by all clients. In the advent of Bitcoin almost 15 years later, PoW proved to be an energy consumption nightmare, as the race for mining profits began. In 2012, the total performance of the Bitcoin network surpassed that of the most productive supercomputer in the world [22]. PoW protocols are slow [19]. The scarce resources required by PoW are CPU clock cycles and electricity [23].

To modify a block relying on PoW, an attacker or a would-be-abuser needs to mine all blocks prior to the one the attacker wants to alter. The cost of mining an individual block is exceptionally high since it is subject to computationally very costly operations, such as solving complex cryptographic puzzles. However, the high computational cost associated with the PoW paradigm is also the main drawback of the blockchain approach used in the context of Bitcoin. The required complexity associated with mining a block requires enormous amounts of power and computation resources, making the approach unsustainable in fields where scale is a concern. For fields such as online advertising, where scale is of great concern, PoW is not a suitable paradigm, even for early-stage implementations.

The challenge of blockchain consensus, which the PoW paradigms attempt to address, is that the distributed system must agree on a single shared state. The current consensus mechanism designs of blockchain are slow, time consuming and energy inefficient. The most popular alternative consensus mechanism to PoW is PoS. There are many other alternatives to PoW. However, it is unclear how their security properties and incentives hold up in comparison. Alternatives include replacing meaningless crypto-puzzles used in PoW with meaningful problems, or making power consumption less wasteful [24]. The main consensus mechanisms are PoW, PoS, delayed PoW (dPoW), proof-of-burn (PoB), proof-of-capacity (PoC), proof-of-activity (PoA), proof-of-existence (PoE), proof-of-intelligence (PoI), proof-of-luck (PoL), ripple ledger, lightning network, and cross blockchains. Detailed descriptions of the consensus mechanisms listed above can be found in [18].

D. ON-CHAIN, OFF-CHAIN AND SIDECHAIN TECHNOLOGIES

There are three different system architecture components that can be used when designing a blockchain-based solution. The three basic ideas are presented in Figure 2. Information into a blockchain can be entered on-chain (a) directly. Alternatively, information into a blockchain can be entered (b) indirectly, via an off-chain insertion. There can also be a trust relationship between a parent and a sidechain (c). Off-chain and sidechain concepts are explained in more detail in the following paragraphs.

Sidechain is a blockchain that can validate data from other blockchains [26]. Sidechains extend the

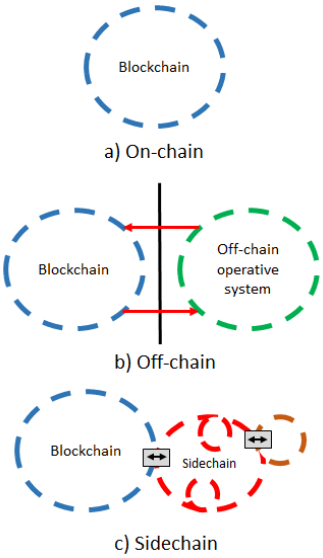

FIGURE 2. The basic idea of on-chain, off-chain, and sidechain, adapted from [25].

decentralization of trust to other digital assets. A sidechain is a separate blockchain attached to the parent. Sidechains are attached to the parent chain with a two-way peg [27]. The idea of a sidechain is to avoid unnecessary trust on top of the parent chain [26]. The processing of transactions can also take place in permissioned and private sidechains, allowing transactions from one chain to be used in another separate chain and vice versa, securely. Sidechain is a more efficient and flexible consensus mechanism with substantially less significant nodes [28]. Such interoperable chains are called pegged sidechains [26]. Sidechain technology has been implemented to established blockchain platforms, but there are still challenges [27].

Off-chain applications provide real-time, verified transactions to all users of the application without transaction fees by committing transactions between users in a separate ledger [29]. Off-chain transactions have serious risks. Most off-chain systems require that the users trust them. An off-chain system could be hacked, leading (among other things) to economic losses [29]. It should be carefully considered when to use on-chain or off-chain transactions, as both have pros and cons. There are tradeoffs with both [29].

Distributed applications include a full application stack for accessing blockchains and off-chain solutions like databases and storage. Nowadays it is possible to store the records in a blockchain with smart contracts [28]. Depending on the smart contract solution, there are different rules for when to store in the chain, what kinds of records are stored, and what the data being stored is. Smart contracts usually use API interfaces to communicate with off-chain applications, allowing off-site data utilized efficiently [28].

Regardless of the way data is created, off-chain or on-chain errors affecting accuracy can occur in both single and multiple chain architectures. The inaccuracies in a blockchain are not easy to overcome. In a private and permissioned chain, the risk of a single party gaining the majority of the tokens is higher. For instance, a concentration of nodes, adding a significant computing power altogether, could create collusion that affects trust, which is the basis of the blockchain technology [30].

E. ENERGY EFFICIENCY AND BLOCKCHAIN

To become as secure as Bitcoin, alternative blockchains must secure their network with equal hashing power. This is neither economic nor energy efficient [31]. One way to increase energy efficiency is to use an approach created by Gridcoin. Instead of crunching arbitrary numbers, the extensive processing power could be used for more practical tasks, such as in the case of online advertising, to validate whether a visitor is human or not in order to mitigate rampant fraud [32]. As there is little available data on the power consumption of alternative blockchain implementations with a scale even near Bitcoin, we have analyzed the energy consumption of Bitcoin PoW as a reference point for future solutions.

Bitcoin mining uses 982 MWh/day, which transforms into an energy cost of $15 million [12]. According to [33], energy consumption per Bitcoin was 240 kWh in 2014, and it has increased since then. Energy costs are paid in traditional currency [33]. There are cryptocurrencies with better energy efficiency, such as Mintcoin [34]. The average monthly growth of the Bitcoin network hash rate has been 37%, but it has slowed down as the price of Bitcoin has grown. The current growth rate leads to continuous energy consumption, which varies between the output of a small power plant and the total energy consumption of a small country, such as Denmark. In 2015, the Long Future Foundation presented a modeling tool showing that Bitcoin could one day consume up to 60% of global energy production, or 13000 TWh. Even in a conservative scenario of a 5% year-on-year growth, with half of the energy from fossils, over 4000 kg of CO2e per mined Bitcoin is produced [35]. In comparison, the average person creates roughly 5000 kg of CO2e per year. In September 2017 the blockchain size was 125GB, and it grew by 35GB from September 2016 [36].

Recently, algorithms requiring more powerful mining techniques have been taken over by ASICs, cloud mining, and mining pools [19]. An ASIC miner can have a hash rate of 30 Ghash/s compared to 0.5 Ghash/s in 2013. According to [23], the average mining energy efficiency from 2010 to 2013 was 500 W per Ghash/s [23]. The best modern ASIC mining solutions consume 0.5-0.6 W per Ghash/s of power, resulting in an average energy efficiency of 0.9-1.0 W per Ghash/s [37]. The technological advancements among chip makers and hardware manufacturers ensure Bitcoin miners are likely to become more than three times as efficient, but Bitcoin usage is growing faster than the technology advances [38].

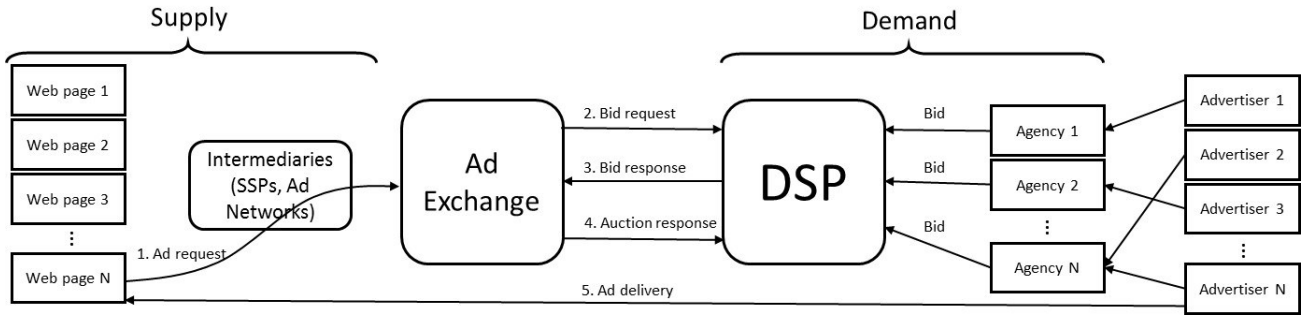

FIGURE 3. Online advertising ecosystem.

IV. SPECIFIC REQUIREMENTS RELATED TO ONLINE ADVERTISING

The online advertising ecosystem has many stakeholders between the advertiser and the web page requesting an ad. Typically, a publisher leases ad spaces to an ad network. When a user connects to a web page with ad spaces, an ad request is generated. The request is typically passed to the ad network, which in turn can forward it to other ad networks or the Supply Side Platform (SSP), passing through many intermediaries before arriving at the Ad Exchange. The process until this point is called the supply side.

The Ad Exchange proceeds to a bidding process. This part of the process is called the demand side. The standard for a bidding process is the open real-time bidding (RTB) protocol. An Ad Exchange generates a bid request according to the openRTB standard [39]. The bid request is forwarded to the Demand Side Platforms (DSPs), which are registered in the Ad Exchange in question. The DSPs configure programmatic advertising campaigns. When a bid request is received, the DSP verifies a match to the configuration parameters of any of its ongoing campaigns. If there is a match, the DSP generates a bid response with the price the advertiser is willing to pay to display its ad on the web page. The latency of bid responses to a given bid request received by the Ad Exchange must be less than 100 ms [40]. The Ad Exchange runs an automated auction and informs the selected winning bid to DSPs. The Ad Exchange coordinates the delivery of a URL of the ad, which is downloaded by the web browser. A delivered ad is referred to as an ad impression. This whole process is presented in Figure 3.

The technology requirements for an online advertising specific implementation of blockchain fall into two categories: online advertising specific requirements and general requirements for blockchain. The general requirements for blockchain include scalability, inability to modify blocks, and energy efficiency. Online advertising specific requirements are based on the assumption that blockchain implementations should be able to address the significant challenges in online advertising: privacy, ad fraud, and lack of transparency. In a public statement in May 2017, David Weldon, the president of the World Federation of Advertisers and the CMO of Barclays Bank, said that a reform leading to a safe and transparent marketplace is the ''only future online advertising has'' [41].

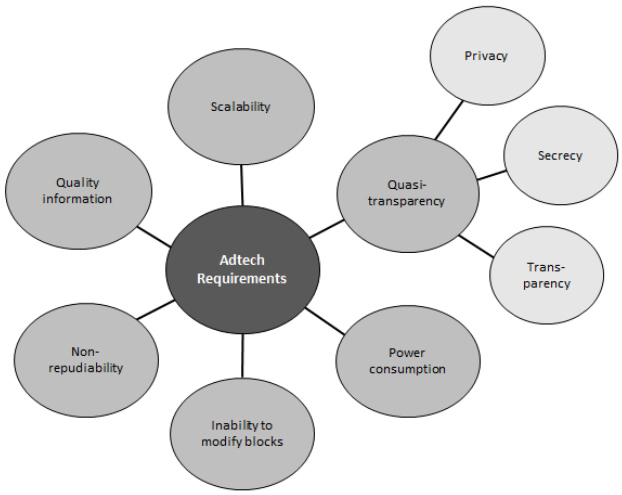

FIGURE 4. The requirements of online advertising to blockchain technology.

Examples of ad fraud include advertisers paying for advertising space not seen by consumers [42], traffic that is generated by bots, and other means. All programmatic impressions can be exposed to ad fraud [5]. The amounts of fraudulent ad impressions vary between 15-30% [43], [44] and result in an economic loss of 20% of total digital ad spend wasted [42]. The situation is similar across video and banners. In 2014, the Association of National Advertisers (ANA) reported that 23% of video views are fraudulent [43]. Ad fraud is approximated to grow to $50 billion by 2025 [5]. Transparency issues aggravate ad fraud. Almost 30% of the top 5000 websites use privacy solutions that prevent the possibility to connect the website to any individual or company for media buyers [5]. Other transparency challenges include lack of pricing information, black box bidder strategies, and masked inventories [45].

Our proposed requirements address the above challenges from a technical point of view. In the following chapters, we will provide an overview of the requirements presented in Figure 4.

A. SCALABILITY

In the context of blockchain, scalability is understood as the number of nodes able to participate in a blockchain. The block generation rate has received far less attention. In other words, current blockchain implementations focus on on-demand authentication of transactions as opposed to managing a stream of transactions. While there are proposals for approaches claiming to scale to hundreds of millions of nodes, none of the existing models claim to address the issue of scalability regarding the number of transactions at the scale of services, such as online advertising. In the programmatic online advertising ecosystem, thousands of intermediary companies are helping advertisers place ads on millions of websites. These ads target billions of Internet users [46] and result in up to a trillion daily transactions. This ecosystem requires massive scalability from the solution serving it. In the online advertising context, a specific stakeholder performs in the order of tens of millions to tens of billions of transactions per day; rates of hundreds to hundreds of thousands of transactions per second. Moreover, these blocks need to be created in real time. Blockchain research and development does not have an understanding of dealing with this kind of volume. Existing proposals envision much lower rates of block generation and fail to meet the demands of online advertising.

In the previous paragraphs, we have discussed scalability related to the generation of blocks. However, a complementary problem is the validation of blocks. If validation is done off-chain, the scalability demand of the system is lower. However, if the validation is expected to be done in real-time, the challenge is enormous, as chains need to be distributed in near real-time to all nodes in the network so that they can validate the blocks. Once the scalability requirements of online advertising are resolved, blockchain has the capabilities for implementation in almost any vertical industry or scientific application.

B. QUASI-TRANSPARENCY

Online advertising-related transactions require anonymity; whereas typical blockchain based systems do not. Whilst typical blockchain systems expose information about nodes, an online advertising implementation needs to protect it. Every transaction must provide privacy, secrecy, and transparency, all at the same time, for different data sets inside the transaction. Privacy relates to the Internet users' rights and ability to protect their data, and secrecy to the advertising actors' need to keep sensitive trading data secret. Transparency requires the availability of relevant information for rational decision making, in contrast to hidden agendas and conditions [47]. For example, information that helps advertisers to reduce their exposure to fraud or brand safety threats, or information that helps Internet users understand why particular ads are shown to them. The lack of transparency may affect the advertisers' interest to buy online advertising as a result of creating an unreliable marketplace [46], [47].

Conceptually, in blockchain protocols, the blocks form a distributed database, including information about the transactions. The information is public for all nodes in the network. However, this principle is not suitable in the online advertising marketplace. The information recorded in each transaction is considered sensitive by the creator of the block. It might, for instance, include financial information related to the transaction, the name of the publisher, and the name of the advertiser. Specific factors such as protecting children [42] should be considered regarding data protection. Therefore, to develop a blockchain protocol suitable for the online advertising industry, irreversible anonymity of sensitive information included in a transaction is a business-critical feature. This requirement is not specific to online advertising and has far-reaching potential across a multitude of fields where authenticity is required, but sensitive information cannot be compromised.

C. INABILITY TO MODIFY BLOCKS

The challenges in online advertising ecosystems often relate to the various intermediaries operating with proprietary technologies, at times preventing advertisers from assessing the quality of advertising campaigns [46]. As it stands, advertisers are left dependent on the reporting from their Ad Network, DSP, agency partner [46], or third-party verifiers. Blockchain protocols respond to the need for creating trustless systems where there is no need for third-party verification of any kind. One of the fundamental properties guaranteeing trust is the inability of nodes in the network to modify created blocks. In the case of Bitcoin, this is achieved through the proof-of-work paradigm. Unfortunately, proof-of-work does not scale to billions of transactions per day needed in the online advertising context. Alternative solutions need to be explored. In the case of online advertising, we call for a blockchain technique where, without moving fundamental transactional aspects off-chain, or otherwise impeding the ability to evaluate individual transactions later, the inability to modify blocks is guaranteed. This is done while meeting the scale demand as per the requirement of 10^11 to 10^12 transactions per day.

D. NON-REPUDIABILITY

The requirement of non-repudiability is a fundamental property defining the concept of trustless systems. This property can be guaranteed with current blockchain technology, but is only meaningful in cases in which the important transactions are in the blockchain. Many of the reviewed implementations in Table 1 show that this is not the case with online advertising implementations; actual transactions are handled off-chain. In a trustless system, a node making a transaction should provide proof of identity together with information such as the date of creation of the block, unequivocally linking the associated identity and transaction to the block. The result is that a node cannot repudiate the associated transaction to the block. Unless important transactional information is stored in the block, as opposed to being stored off-chain, the proof of

TABLE 1. A comparison of Adtech-related blockchain solutions.

Factor	Adchain	AdEx	BAT/Brave	NYIAX	Madhive	Papyrus
Description	Ethereum-based platform for decentralized applications for the digital advertising ecosystem	Ethereum-based ad exchange for online advertising addressing fraud and privacy.	Token of exchange in a secure, anonymous, opt-in advertising system based on the Brave browser	Financial trading and advertising technology combined	Blockchain-based ecosystem dedicated to advertising	Decentralized advertising ecosystem
Proof methodology	Modified PoS	PoS	Zero-Knowledge proof	Proof-of-Asset	Byzantine fault tolerance	PoS
Off-chain	No	Yes	Yes	Yes	Yes	Yes
Sidechain	Yes	No	Yes	Yes	Yes	Yes
Two-way peg	Yes	No	Yes	No	No	No
Open source	Partly	Yes	Yes	No	No	Yes
Scalability trans./sec	Only whitelisting of domain names	Trans. off-chain	Latency issues	Batch processing, non-real-time	Transactions logic off-chain	> 1M
Quality information	Whitelist	Yes	Yes, attention score	Yes	Yes	Yes
Non-repudiability	Authentication of nodes with TSL	Proof-of-conversion and User ID	Yes	Yes	Yes	Yes
Quasi-transparency	No	Yes	Yes	Yes	Yes	Yes
Inability to modify blocks	Partly	Yes	Yes	Yes	Yes	Yes
Power consumption	Ethereum-based	Ethereum-based	Ethereum-based	No data	Proof-of-Real-Work	No data
Released	Jul 17	Feb 18 Beta	May 17	Mar 17	Apr 16	Mar 18
Adaptation	Low	Low	Low	Low	Low	Low
Reference	[52]	[53]	[8], [67]	[59]	[30]	[11]

identity loses its value. The proof of identity is as valuable as the information associated with it.

E. QUALITY INFORMATION

One of the challenges of online advertising is how, after starting a campaign, advertisers have little control over how their ads are displayed and to which audiences their ads are shown. Advertisers lack methods for reliably verifying the placement of their ads. As a result, ads may end up adjacent to undesirable content [42]. As it stands, the best-established quality standard, known as viewability, measures whether the user sees at least 50% of the ad for at least a second [46].

In addition to the demand for scale, its dependence on quality information makes the technical requirements of an online advertising blockchain implementation challenging. It is not enough to merely consider the transactional benefits, namely authenticity of transactions. Examples of quality information include whether the ad viewable, whether a human is viewing it, and whether the placement of the ad is relevant and appropriate. Quality assessment can take place at four different levels: a publisher (a company), a website, a page on a website, and the user who sees the ad. There is also the consideration between deliveries, such as whether the ad is viewable and whether a human sees it, and value, which is concerned with return-on-investment (ROI). Whereas delivery focuses on assessing – as a binary statement – whether there is potential for ROI or not, value focuses on assessing how much of that potential there is.

The potential value of ad placement and the associated risks are still poorly understood and need consideration in the context of blockchain implementations. The basic premise is that whatever quality information is seen as essential is encoded as part of each created block. A problem stems from the fact that in most cases it cannot be the advertisers' conduits that generate such information, but it needs to be an implicit product of their activity. Understanding and clearly defining such implicit information and how to create it is a complex problem, which is complementary to the outline of a blockchain protocol discussed in this document.

F. ENERGY EFFICIENCY

The energy efficiency problem is not sufficiently handled in the computer engineering field at present [48]. In practice, electricity and environmental costs are hidden in our society [49]. The environmental impact of online advertising is multidimensional. We presume that online advertising consumes significant amounts of energy even without blockchain, leading to the production of substantial CO2e emissions. The always-on online advertising ecosystem uses power based on the premise that related systems depend on 24/7/365 low-latency availability, in order to facilitate real-time transactions at a notable scale. Currently, there is no

clear understanding of the energy efficiency of online advertising solutions, and it remains challenging to approximate actual power consumption.

Energy efficiency and consumption are not requirements specific to online advertising. Energy efficiency concerns the whole blockchain technology, hashing procedures, and mining. The energy consumption of Bitcoin, which is PoW-based, has been widely acknowledged. It should be noted that Ethereum, the primary alternative for Bitcoin, whilst more energy efficient, uses an estimated 19.57 TWh of energy yearly – close to the energy consumption of Iceland [50]. Most of the available blockchain-based solutions for online advertising are based on Ethereum.

Growing energy consumption is a global problem. In many cases, the ICT industry enables substantial energy savings in other industries through automation, for example. It must be a requirement for any ICT solution nowadays not to consume excessive power or emit additional CO2e to burden the environment in any circumstances. Online advertising is no exception. A comparison should be made between the blockchain solutions and their substitutes. Power usage is one of the many competing optimization factors, unfortunately in many cases overdriven by economics, resiliency, scalability, security, or quality. Transparency of energy consumption data regarding different solutions is low or nonexistent. More focus on energy consumption is needed from researchers and the industry. For these reasons, we consider energy efficiency a requirement for a blockchain-based online advertising solution.

V. REVIEW OF BLOCKCHAIN PLATFORMS AND IMPLEMENTATIONS IN ONLINE ADVERTISING

There are many blockchain platforms already available. Developers have implemented various blockchain-based technologies; file storage, communications, file serving, archiving, data processing, bidding, predictions, and recently, online advertising and many other critical digital economy capabilities. We will focus on platforms which provide support for distributed application development. We have selected a set of platforms from those available based on popularity. We also seek a varied selection of different kinds of platforms to get an overall picture of the available platforms. There are many blockchain-based solutions under development that are directed at supporting the online advertising ecosystem. We selected the most popular and platforms with the greatest potential. Section A analyzes blockchain platforms and Section B the solutions created for online advertising.

A. ANALYSIS OF ONLINE ADVERTISING VERTICAL BLOCKCHAIN SOLUTIONS

Blockchain technologies promise to offer solutions to transactional systems. No well-established blockchain-based application for online advertising has been implemented as of Q2/2018. We conducted a thorough literature review and industry analysis. We did not find any academic papers, only one technical disclosure of blockchain verification on the online advertising ecosystem [51] and several industry white papers. One industry body has been established to guide online advertising companies regarding blockchain [10], but nothing has been published by them to date. Several commercial entities have made proposals or actual proof of concept implementations of blockchain in the online advertising context. We analyzed the following solutions: AdChain, AdEx, Comcast blockchain, Basic Attention Token (BAT)/Brave, NYIAX, Madhive, and Papyrus. In the following paragraphs, we will explain and analyze solutions on a more detailed level. BAT/Brave and Adchain have the most comprehensive white papers that are publicly available. Results of the analysis of all solutions are presented in Table 2.

Adchain/Adtoken is the second online advertising network to leverage the Initial Coin Offering (ICO) funding scheme, one wherein cryptocurrency tokens are sold in an initial offering in a land-rush style event to raise capital for the company. Adchain is an Ethereum-based blockchain solution for online advertising. It is a decentralized solution and uses modified PoS as consensus. AdChain does not utilize off-chain application logic, and it supports sidechains. AdChain is open source, but some of its applications are private. Quality information is based on whitelisting [52]. AdChain does not address transactions. Therefore, scalability to handle online advertising transactions is not relevant. As opposed to the model introduced by BAT, Adtoken (ADT) cannot be used to buy ads. Instead, advertisers still pay for ads with currency and Ad tokens are used for voting for which sites can be included in the Adchain advertising network. This proposal creates a conflict: if the majority of the token holders are not advertisers, or if advertisers do not take an active role in the voting process, there is potential for conflict of interests. Adopting such a voting mechanism for inventory selection implies that voters have the required knowledge about sites and are incentivized to make decisions that are beneficial for the advertisers' spending money on the network. There is no evidence to suggest either of these is correct.

AdEx is an Ethereum-based blockchain solution, which primarily addresses fraud and privacy issues in online advertising. It is a decentralized system using smart contracts and modified PoS as a consensus. Only critical data is verified and stored on the blockchain. The idea behind AdEx is to create a user profile web page, which allows the user to select exciting advertisers on a voluntary basis. This mechanism is called whitelisting. Users also voluntarily provide more specific information on their interests to these favorable advertisers in order to receive highly targeted ads [53]. AdEx does not support off-chain functionality. AdEx does not use blockchain for individual transactions. Therefore, the scalability requirement can be fulfilled. New solutions, which require end-users to be active in taking the solution into use, face challenges of

TABLE 2. A comparison of blockchain platforms.

Platform	Description	Proof methodology	Off-chain	Sidechain	Two-way peg	Open source	Scalability trans./sec	Reference
Bitcoin	Crypto-currency platform	PoW	Yes	Yes	Yes	Core, Yes	6.8	[36], [62]
Ethereum	General purpose crypto-currency platform that runs smart contracts	PoW, PoS	Yes	Yes	Yes	Yes	25	[57], [64]
Ripple	Enterprise blockchain solution for global payments	PoW-based Ripple protocol consensus	Yes	Yes	Inter-ledged	Yes	1000	[19], [23], [65]
Counterparty	An overlay protocol of currency assurance and exchange	PoB	Yes	No	No	Yes	No data	[66]
OmniLayer	Financial derivate platform	Overlay on top of Bitcoin PoW	Yes	Yes	Yes	Yes	13000	[67], [68]
Open Transactions	Untraceable and anonymous transactions without latency	PoW-based	Yes	Yes	Yes	Yes	No data	[69]
BitShares	Decentralized crypto-equity share exchange	Delegated PoS	Yes	Yes	Yes	Yes	100000	[70], [71]
ColoredCoins	Provides Bitcoin asset marking for digital/physical assets	Proof of ownership	Yes	No	No	Yes	1M-25000Bn*	[72], [73]

* Based on Lightning Network

broad adaptation. AdEx is an open-source solution, which is promising for the future development.

Comcast is developing a blockchain-based platform with Disney, Channel 4, NBC, and several other large cable TV companies. The solution uses blockchain to share information securely between the consortiums. The solution lets members share marketing data encrypted in a way that allows each member to ask marketing questions from other members' tracking data without exposing all the information. Sharing marketing data improves targeting precision and analytics. The Comcast blockchain solution is operating at the campaign scale. There is no information about the technical specifics of the solution, but with a consortium of powerful companies, expectations are high [54]. The Comcast solution is not going to revolutionize the whole online advertising industry; instead it targets cable TV markets. We will exclude the Comcast platform from the comparison in Table 2 as the necessary data is not available.

BAT is an example of innovative vertical applications of proof paradigms. The BAT model is associated with the Brave browser. BAT introduces a model resembling the original online advertising paradigm, where there are no intermediaries and the entire supply-chain is transparent. In BAT, the advertiser pays for the attention of the user, and the user who contributes their attention is paid in return. The user divides their earnings between different publishers. In BAT, all user-related privacy data is kept in the end-device. Tracking is performed locally with a local machine-learning program, and transactions toward exchange servers can introduce excessive latency compared to the requirements of online service responsiveness. In addition, a broad scale adaptation requires end users to change behavior and adopt a new browser, which may prove to be a challenging goal to achieve [8].

We propose that this model can be improved by directly dividing the money between publishers and users, in a similar way to which money is typically shared between publishers and various intermediaries. Instead of channeling tokens to the publishers, the user will then have the option to choose from a variety of national charitable causes and decide how the earned funds will be allocated to those charities. Providing the publishers with the majority of the tokens associated with each advertising event could alleviate concerns that Brave's new model has already created [55].

Another challenge in the BAT model is the introduction of a token as a currency for advertising, instead of using conventional currency. This creates a feasibility problem, where acquiring the token becomes an obstacle for adoption. For example, if an advertiser or their media agency representative would want to advertise on the BAT network, they would first have to buy USD (or EUR) using local currency, and then convert that into Bitcoin (BTC), which then would have to be converted into Ether (ETH). With ETH, it is possible to acquire the tokens required to transact in the BAT network. Each step of the conversion involves a commission and a significant cognitive overhead – mostly associated with uncertainty. Furthermore, there are trust issues related to crypto-currency platforms; cases range from minor concerns to token or cryptocurrency holders losing their holdings entirely.

Some of the most significant cases eroding trust in cryptocurrencies include the Mt. Gox bankruptcy [56], the events leading to Ethereum's "hard fork" [57], and the general quality issues in the Bitcoin ecosystem, most notably those

burdening coinbase.com [58], the leading Bitcoin platform. There are also significant concerns related to the volatility of crypto-currencies and solution-specific tokens, such as BAT. Given the high level of deliberation that goes into budgeting among advertisers, cryptocurrencies as they stand today are not a suitable option for large-scale media investment. Finally, cryptocurrencies are not regulated in any way and are therefore prone to the kinds of manipulation, which can cause suprises for unprepared media investors.

NYIAX is a spinoff from NASDAQ. It utilizes the capabilities of financial trading combined with advertising technology. NYIAX is a platform that enables publishers and advertisers to buy, sell, and re-trade premium advertising inventory. NYIAX uses proof of asset (PoA) as a consensus, and some of its application logic is off-chain. Sidechains are also supported, and the solution can also be integrated with other solutions. NYIAX is not an open source project. Its scalability is ensured by processing transactions in larger batches in non-real time. As a stock exchange-based solution, one of the key strengths of NYAIX is confidentiality and security, on top of financial transactions [59].

The MadHive blockchain-based solution is designed for the advertising industry. It provides a trusted connection for data exchange and collaboration between adtech stakeholders. Madhive uses Byzantine fault tolerance as a consensus. Scalability is achieved with part of the application logic and transactions residing off-chain. It does support side-chains. The Madhive solution ensures quasi-transparency. Off-chain trust is built on encryption and a crypto key server. The client, order details, and performance data are encrypted. The MadHive follows a PoW protocol in which the cryptographic puzzle is replaced with a real-world ad-related puzzle. Therefore, the energy efficiency of a MadHive solution is improved. MadHive has customers, and the platform is commercially available, unlike many other solutions described in this review [30].

Papyrus is a decentralized solution for online advertising. It is an Ethereum-based blockchain solution with smart contracts, and it uses PoS as consensus. According to [11] Papyrus is developing state channel technology to ensure scalability to billions of transactions daily. The solution is similar to Raiden Network and Lightning Network. Papyrus uses RTB as the basis for the solution design, to address the dominant existing technology and fast adaptation. Papyrus is decentralized data storage. It supports off-chain and sidechain technologies, and it is an open-source project. Papyrus informs scalability to over 1 million transactions daily. The actual scalability is far from what is required to become a standard solution in the adtech market. Identity verification ensures quasi-transparency, and every smart contract has an ID.

As a summary, there are two approaches that represent a different paradigm; currency-token-ads and currency-token-control. Whereas in the currency-token-ads model advertisers exchange tokens directly with alleged user attention, in the currency-token-control model, at least in the case of Adtoken, the main issue is how a site can earn legitimacy by owning enough tokens and how it can use it to act in their interests and against the interests of the broader marketplace. Because the entire market capitalization of Adtoken is less than $25 million [60], manipulation is straightforward for bigger malicious players; it has been suggested that the most significant reported ad fraud make more in a single week [61].

These early examples leave essential questions unanswered. The critical issues we have identified in these proposals can be categorized as financial and technical. The financial concerns are related to the cost and relative difficulty of converting regular currency to cryptocurrency and tokens, the volatility of crypto assets, the risk of marketplace manipulation due to concentrated token ownership, and the absence of regulation. The technical concerns include marketplace complexity, scalability, transaction delays, and blockchain transparency benefit being lost due to moving critical functions off-chain.

Most of the blockchain-based solutions available for the online advertising ecosystem are based on Ethereum. Next, we will investigate the alternatives for Ethereum.

B. REVIEW OF BLOCKCHAIN PLATFORMS

We have analyzed the following platforms: Bitcoin, Ethereum, Ripple, Counterparty, Omni, Open Transactions, BitShares, and Colored Coins. In the following paragraphs, we will provide a brief outline of these platforms.

Bitcoin is the oldest and most widely used blockchain platform. It uses PoW as a consensus. Bitcoin supports off-chain and sidechain technologies with a two-way peg. The core of Bitcoin is open source, but some of its components are not. Bitcoin currently scales up to 6.8 transactions per second. It is a secure decentralized platform [36], [62]. Bitcoin is not a feasible platform for online advertising purposes, mainly due to its lack of scalability.

Ethereum is a blockchain-based decentralized multipurpose cryptocurrency platform, which runs smart contracts. Smart contracts are applications that run precisely as programmed without any downtime, censorship, fraud, or third-party interference. In the case of downtime and third party interference, both claims have recently been brought into a discussion [57], [63]. Ethereum is a stateful platform [64] and includes a programming language that allows users to create decentralized applications. There is a range of applications based on smart contracts.

Ripple [65] provides a total solution with a gateway, a payment solution, an exchange solution, a remittance network, and a smart contract system. The Ripple network provides a globally shared ledger, which assigns applications authoritative information about the state of accounts and creates a new ledger in seconds. The Ripple network contains many distributed nodes, which process transactions. Client application transactions are relayed to the entire network [23]. Ripple enables decentralized server architecture for the movement of value among financial institutions. Ripple allows member companies to make payments directly to each other [19].

Unfortunately, the energy efficiency of Ripple is as bad as that of PoW.

Counterparty is a decentralized Bitcoin-based platform that was developed to provide enhanced features on top of Bitcoin software. The protocol is open source and well tested. Counterparty provides the creation and trading of any digital token, writing digital agreements, and executing data into the Bitcoin blockchain. Counterparty uses proof of burn (PoB) as a consensus. It supports off-chain application logic. The Counterparty is an open source project. No scalability data was found from public sources [66].

Omni is an open-source financial derivatives blockchain platform. It is a decentralized blockchain platform on top of Bitcoin blockchain. It is a software layer. The primary purpose of Omni is to create and trade digital assets and currencies. The main functionalities of Omni include custom currencies, a crowdfunding capability, a secure wallet, and an integration server daemon for easy integration to external systems. Omni uses Bitcoin PoW as consensus. It reports scalability of up to 13000 transactions per second [67], [68].

Open Transaction is a decentralized open source blockchain platform. Transactions in Open Transaction are unforgeable, receipts are destructible, and balances cannot be falsified or changed without user consent. Transactions are untraceable and anonymous without latency. It is an overlay technology on top of Bitcoin and uses PoW as a consensus. Open Transaction supports off-chain and sidechain technologies. No scalability data is available on public sources [69].

The BitShares platform is an open source decentralized blockchain-based platform providing smart contracts. The core features of BitShares are a high-performance decentralized exchange, cryptocurrencies, and smart contracts. It reports scalability to 100000 transactions per second. BitShares uses delegated PoS as a consensus. Delegated PoS utilizes stakeholder approval voting to achieve consensus in a fair and democratic way. BitShares supports off-chain and sidechain technologies [70], [71].

Colored Coins is a method for transferring metadata to the Bitcoin blockchain and a platform for cryptocurrencies. It is an open-source platform. Colored Coins utilizes Bitcoin and is integrated into Lighting Network. Colored Coins uses proof-of-ownership (PoO) as a consensus. It supports off-chain application logic but not sidechains [72], [73]. The Lighting Network [73] has some benefits: instant payments, no confirmation times, smart contracts security off-chain, and scalability of millions to billions of events per second. The Lighting Network achieves low cost by transacting off-blockchain and by leveraging instant micropayments. Instant micropayments are suitable for real-time bidding (RTB). Cross-chain atomic swaps can occur off-chain instantly with various consensus rules. The Lightning Network comes the closest to meeting the scalability requirements of online advertising.

VI. RESULTS

We raise the vital question of whether any of the blockchain-based solutions available for online advertisers offer a viable solution for the five critical challenges presented in Section 4. None of the solutions have the market adoption to suggest significant buyer confidence. No commonly agreed standard or dominant design has yet been formed.

A. RESULTS OF ONLINE ADVERTISING VERTICAL BLOCKCHAIN SOLUTIONS ANALYSIS

In addition to blockchain platforms, we analyzed vertical solutions designed especially for online advertising against the requirements presented in Section 4. The results are presented in Table 1.

Data was gathered from public sources. There are uncertainties in the data, as many of the solutions are in the very early phases of development, or market adaptation is low. Three of the solutions were Ethereum-based, and therefore inherit the basic properties of Ethereum. Power consumption data was not available in any of the solutions; it was as if it had no relevance. In respect to the requirements presented in Section 4, it is too early to say which of the solutions, if any, are the most promising. None of the existing solutions have even moderate market adaptation. Therefore, making an evidence-based judgment is not possible with regard to whether any of the solutions will eventually work or not. Alternatives to existing solutions can come from selecting another blockchain platform. We will present a summary of the blockchain platforms in Section B below.

B. RESULTS OF BLOCKCHAIN PLATFORM ANALYSIS

To find solutions that meet the requirements presented in Section 4 and to address the challenges of ad fraud, we analyzed the main blockchain platforms. The results are presented in Table 2.

All of the analyzed blockchain platforms had a somewhat different proof method. In addition, all platforms have capabilities to perform transactions and enrich data off-chain. We did not find any evidence of sidechain support for Counterparty and Colored Coins from public sources, even though they operate as sidechains themselves. Off-chain processing is needed for scalability, but at the potential cost of losing the authentic security of blockchain. As they are off-chain, they are software, making them interesting targets to exploit. All of the analyzed platforms relied on open source and had a community developing the entire platform, or at least parts of it. The best-suited platforms that have the potential to meet the requirements of online advertising were BitShares and Colored Coins. Colored Coins is based on Lightning Network technology, which promises scalability to billions of transactions daily. The fit for online advertising is not 100%, some compromises regarding the requirements must be made. Another finding is that the platforms relying on pure PoW do not scale to online advertising without a significant part

of the application logic being off-chain. Once the main part of the application logic is off-chain, it contradicts the initial benefits of the blockchain. Solutions utilizing Colored Coins could have the potential to scale to the requirements of online advertising. None of the investigated vertical solutions for online advertising are currently based on Colored Coins.

C. VALIDITY OF THE RESULTS

The presented requirements address the widely known challenges of online advertising and ad fraud. Even though blockchain as a technology is known, no scientific articles have been written about its scalability or other key features necessary for online advertising. The results regarding blockchain platforms are novel, and therefore they can be taken to a more detailed level once a blockchain platform is processing transactions at massive scale and actual transparent data on the performance of the solution is provided. The blockchain is known for its notorious power consumption, as miners are processing mathematical tasks with no other meaning than ensuring valid transaction. As more nodes join the chain, the situation worsens.

Blockchain-based solutions for online advertising have not been investigated in scientific articles before to the best of our knowledge. The presented data relies on commercial information sources and can contain promises without actual evidence on the delivery of those promises. Nevertheless, it is the only available information source on the matter, suggesting that more transparency, development, and research is needed in this field to get performance and quality data from operational implementations. The suggestions and discussions for future development and research in Section 7 are based on the industrial and technical knowledge of the researchers and can be considered a guideline for meeting the requirements in future system designs.

VII. DISCUSSION

In terms of the requirements presented in Section 4, after a comprehensive review of blockchain platforms and blockchain-based solution for online advertising, we suggest ideas for consideration in future system designs.

A. SCALABILITY

To achieve the required scalability, approaches such as PoW or PoS are not feasible options, since both act as a cause of delay even in relatively low-scale environments. A proof concept capable of realistically meeting far higher demand for scale is mandatory. An initial approach along these lines has already been proposed [24]. However, each node can create parallel chains at speeds defined by its transaction rate. Unfortunately, guaranteeing nodes cannot modify blocks at such rates. It is an open challenge that needs to be carefully considered. In the referred proposal, the authors suggest using timestamps as a reference of the instant creation of the block in such a way that the block n in the chain has to be created before block n + 1, but later than block n-1. This is an interesting approach; however, it needs to be carefully evaluated in the context of different problems (e.g., transactions generated in parallel, and the desynchronization of computer clocks). Moreover, in-depth analyzing should be performed to conclude whether it would be sufficient to offer security guarantees equivalent to PoW, which, while not affected by security issues [74], can be considered the best standard proof. Scalability in current solutions is achieved by placing the transaction-intensive part off-chain. In our opinion, this is a compromise that jeopardizes the core benefits of blockchain and is not an acceptable way of solving the scalability requirement of online advertising.

In the case of block validation, solutions based on PoW, which can ultimately be reduced to a competition to create the next block, rely on achieving consensus among the nodes in the network to choose which of the possible blocks is the valid one. In our proposal this is not the case, since each node would be able to generate its chain, avoiding the need for consensus algorithms to be implemented. In other words, we are proposing an alternative paradigm, ''trust without consensus.'' Blocks will be signed by the correspondent node to provide the non-repudiation guarantee.

B. QUASI-TRANSPARENCY

We propose creating a double cryptographic layer for resolving the anonymity challenge. The first one will be like the one defined in standard blockchain protocols, where a node distributes its public key to all other nodes in the network so that anyone can prove the block has been generated by such a node. The second cryptographic layer will take care of encrypting the sensitive information with a second private key of the node. Then, keys able to decipher this information on the second layer will be delivered only to those players the node is willing to let access such sensitive information. Note that this second cryptographic layer can grow in complexity, since there may be situations in which a company wants to provide access to different players depending on the specific transactions. It may still be feasible but it needs to be carefully considered before implementation. In addition, this approach harms the scalability aspect discussed above.

C. INABILITY TO MODIFY BLOCKS

One option to solve the inability to modify the blocks requirement is to limit the time of creation of a block based on timestamps. However, we consider this just a promising scope for future work, we acknowledge that many vital questions remain unanswered, and recognize that it is likely that currently unknown challenges (and solutions) will emerge as the topic is investigated in greater depth.

D. NON-REPUDIABILITY

To solve the non-repudiability challenge, we propose using the cryptographic solutions used in existing blockchain protocols. These approaches use asymmetric public-private key schemes, where the node creating a block signs it with its private key, assuming ownership of the block. On the other hand, the node distributes its public key to the rest of the

nodes in the network so that anyone can verify the identity of the node creating the block.

E. QUALITY INFORMATION

While some of the required quality information may come from Internet users, at least for the time being, there are too many open questions to propose a suitable approach. We propose an incremental approach, where the ultimate goal is that Internet users primarily create all quality information, in a decentralized manner as a by-product of the transactions. As a progression toward this goal, which is still far from feasible considering the lack of theoretical concepts, we propose initially having a collective of independent trusted entities leveraging auditable open source solutions, which generate the required scoring. One example of this would be trading logs that are widely contributed to a pool, and then analyzing them using an open-source platform [75]. The computation of scores would be performed in a separate blockchain. Initially, such an approach could be focused on classifying websites. Quality assessment approaches also need to be considered strictly within the scalability concerns we have highlighted in Section 4.1.

VIII. CONCLUSIONS

We conducted a review of existing blockchain platforms and blockchain-based solutions addressing online advertising. Based on the requirements presented in Section 4, we conclude that none of the solutions evaluated presented any evidence to fulfill the requirements. Barriers to adoption in the broad context include token volatility, scalability, excessive power consumption, trust, and the difficulty of producing reliable quality information.

We provide a rough outline of key considerations regarding the implementation of blockchain in online advertising as an industry-wide adoption. Some barriers can be considered general blockchain problems, and researchers from other fields are also solving them. The requirements related to quality information are specific to online advertising. The focus needs to be directed to this aspect alone, as otherwise various blockchain implementations from eager industry players risk focusing on the transactional aspects or are misguided in their attempts to address issues with an actual value derived from online advertising.

Future research should carry an in-depth description and qualitative analysis of the various blockchain-based online advertising systems. In addition, more research is needed to understand the financial aspect of online advertising and how it relates to blockchain; under which conditions will advertisers and their agency representatives consider significant investments in the token economy? The focus should at least initially be more on the technical challenges, and less on the financial transaction aspect. The promise of blockchain is significant for online advertising and could indeed provide the basis for revolutionizing the industry by basing it on trust and authenticity. Even though there may be faster development on a smaller scale – for example in the case of individual national online advertising markets – the industry could still be a decade or more away from materializing this potential through a global-scale transformation. The global solution must scale without adding a significant amount of resources, and without compromising quasi-transparency, the inability to modify blocks, non-repudiability, quality of information, and energy efficiency. The findings of our research point out that blockchain is not yet ready to be widely implemented in online advertising. In addition to the technical issues that need resolving, the main challenges of online advertising are not well understood by end-users or even online advertising providers. There needs to be a significant awareness campaign to support transformation toward a healthier online advertising ecosystem. In Europe, the General Data Protection Regulation (GDPR) could be harnessed to bring a sense of urgency to change the industry.

REFERENCES

[1] *Paving the Way: How Online Advertising Enables the Digital Economy of the Future*, IHS Technol., London, U.K., Nov. 2015.

[2] PricewaterhouseCoopers. (Apr. 2017). *IAB Internet Advertising Revenue Report: 2016 Full Year Results*. Accessed: Jan. 26, 2018. [Online]. Available: https://www.iab.com/wp-content/uploads/2016/04/IAB_Internet_Advertising_Revenue_Report_FY_2016.pdf

[3] A. Pastor Valles, "An entropy-based methodology for detecting online advertising fraud at scale," M.S. thesis, Universidad Carlos III de Madrid, Getafe, Spain, 2016.

[4] B. Stone-Gross, R. Stevens, A. Zarras, R. Kemmerer, C. Kruegel, and G. Vigna, "Understanding fraudulent activities in online ad exchanges," in *Proc. ACM SIGCOMM Conf. Internet Meas. Conf.*, Berlin, Germany, 2011, pp. 279–294.

[5] M. Kotila, R. Cuevas Rumin, and S. Dhar, "Compendium of ad fraud knowledge for media investors," WFA Global Transparency Group, Brussels, Belgium, Tech. Rep., 2016.

[6] J. Davies. (Mar. 28, 2017). The Gloves are Off: The Guardian Sues Rubicon Project for Undisclosed Fees. Digiday. Accessed: Jan. 8, 2018. [Online]. Available: https://digiday.com/media/gloves-off-guardian-sues-rubicon-project-undisclosed-fees/

[7] D. Tynan. (Aug. 25, 2016). WhatsApp Privacy Backlash: Facebook Angers Users by Harvesting Their Data. The Guardian. Accessed: Jan. 8, 2018. [Online]. Available: http://www.theguardian.com/technology/2016/aug/25/whatsapp-backlash-facebook-data-privacy-users

[8] *Basic Attention Token*. Accessed: Dec. 4, 2017. [Online]. Available: https://www.basicattentiontoken.org

[9] AdToken. *The adToken Lunarscape*. Accessed: Jan. 8, 2018. [Online]. Available: https://adtoken.com/

[10] I-COM. *Data Science Blockchain and Advanced Research Subcommittee*. Accessed: Jan. 8, 2018. [Online]. Available: http://www.i-com.org/blockchain-and-advanced-research-subcommittee/

[11] *Papyrus*. Accessed: Jan. 8, 2018. [Online]. Available: https://papyrus.global/

[12] M. Swan, *Blockchain: Blueprint for a New Economy*, 1st ed. Beijing, China: O'Reilly, 2015.

[13] R. Whitwam. (Jul. 6, 2017). NotPetya Ransomware Hackers Want 100 Bitcoins for Decryption Keys. Extremetech. Accessed: Jan. 8, 2018. [Online]. Available: https://www.extremetech.com/internet/251966-notpetya-ransomware-hackers-want-100-bitcoins-decryption-keys

[14] S. Biddle. (Jul. 19, 2012). The Secret Online Weapons Store That'll Sell Anyone Anything. Gizmodo. Accessed: Jan. 8, 2018. [Online]. Available: https://gizmodo.com/5927379/the-secret-online-weapons-store-thatll-sell-anyone-anything

[15] N. Popper. (Jun. 10, 2017). Opioid Dealers Embrace the Dark Web to Send Deadly Drugs by Mail. The New York Times. Accessed: Jan. 8, 2018. [Online]. Available: https://www.nytimes.com/2017/06/10/business/dealbook/opioid-dark-web-drug-overdose.html

[16] A. Greenberg. (Nov. 18, 2013). Meet the 'Assassination Market,' Creator Who's Crowdfunding Murder With Bitcoins. Forbes. Accessed: Jan. 8, 2018. [Online]. Available: https://www.forbes.com/sites/andygreenberg/2013/11/18/meet-the-assassination-market-creator-whos-crowdfunding-murder-with-bitcoins/#65f308673d9b
[17] M. Van Alstyne, "Why Bitcoin has value," *Commun. ACM*, vol. 57, no. 5, pp. 30–32, 2014.
[18] P. Tasca, T. Thanabalasingham, and C. J. Tessone, "Ontology of blockchain technologies. Principles of identification and classification," Cornell Univ., New York, NY, USA, Tech. Rep., 2017.
[19] M. Pilkington, *Blockchain Technology: Principles and Applications*. Cheltenham, U.K.: HAL, 2016.
[20] BlockchainHub. *Blockchains & Distributed Ledger Technologies*. Accessed: Jan. 8, 2018. [Online]. Available: https://blockchainhub.net/blockchains-and-distributed-ledger-technologies-in-general/
[21] I.-C. Lin and T.-C. Liao, "A survey of blockchain security issues and challenges," *IJ Netw. Secur.*, vol. 19, no. 5, pp. 653–659, 2017.
[22] Bytecoin. *Proof of Stake, Proof of Work Comparison*. Accessed: Aug. 22, 2017. [Online]. Available: https://bytecoin.org/blog/proof-of-stake-proof-of-work-comparison
[23] J. Mattila, "The blockchain phenomenon," Book Blockchain Phenomenon Berkeley Roundtable Int. Econ., Berkeley, CA, USA, ETLA Work. Papers 38, 2016.
[24] M. Milutinovic, W. He, H. Wu, and M. Kanwal. (2016). "Proof of luck: An efficient blockchain consensus protocol." [Online]. Available: https://arxiv.org/abs/1703.05435
[25] Blockstream. *Advancing the Art of Blockchain Technology*. Accessed: Jan. 8, 2018. [Online]. Available: https://blockstream.com/technology/
[26] A. Back *et al.* (2014). *Enabling Blockchain Innovations With Pegged Sidechains*. [Online]. Available: http://kevinriggen.com/files/sidechains.pdf
[27] Bitcoinmining. *Sidechains Explained*. Accessed: Jan. 8, 2018. [Online]. Available: https://www.bitcoinmining.com/sidechains-explained/
[28] V. Lemieux, "Blockchain and distributed ledgers as trusted recordkeeping systems: An archival theoretic evaluation framework," presented at the Future Technol. Conf. (FTC), 2017.
[29] RTWire. (Jan. 24, 2015). Off-Chain Transactions. RTWire | Real Time Bitcoin. Accessed: Jan. 8, 2018. [Online]. Available: http://rtwire.com/blog/2015/1/21/off-chain-transactions
[30] Madhive. *Next Generation Data Management*. Accessed: Jan. 8, 2018. [Online]. Available: https://madhive.com/
[31] "Delayed proof of work (dPoW)," White Paper, GitHub, San Francisco, CA, USA, 2016. [Online]. Available: https://github.com/KomodoPlatform/komodo/wiki/Delayed-Proof-of-Work-(dPoW)-Whitepaper
[32] M. Ingram. (Jul. 1, 2015). There's a Ticking Time Bomb Inside the Online Advertising Market. Fortune. Accessed: Jan. 8, 2018. [Online]. Available: http://fortune.com/2015/07/01/online-advertising-fraud/
[33] D. Bradbury. (Apr. 7, 2014). What is the Carbon Footprint of a Bitcoin? CoinDesk. Accessed: Jan. 23, 2018. [Online]. Available: https://www.coindesk.com/carbon-footprint-bitcoin/
[34] Digiconomist. *Bitcoin Energy Consumption Index*. Accessed: Jan. 8, 2018. [Online]. Available: https://digiconomist.net/bitcoin-energy-consumption
[35] F. X. Olleros and M. Zhegu, *Research Handbook on Digital Transformations*. Cheltenham, U.K.: Edward Elgar, 2016.
[36] Bitcoin.com. *Blockchain Size*. Accessed: Jan. 8, 2018. [Online]. Available: https://charts.bitcoin.com/chart/blockchain-size
[37] A. Hayes, "A cost of production model for bitcoin," New School Social Res., New York, NY, USA, Work. Paper 05/2015, 2015.
[38] S. Deetman. (Mar. 29, 2016). Bitcoin Could Consume as Much Electricity as Denmark by 2020. Motherboard. Accessed: Jan. 8, 2018. [Online]. Available: https://motherboard.vice.com/en_us/article/aek3za/bitcoin-could-consume-as-much-electricity-as-denmark-by-2020
[39] IAB Technology Laboratory. *OpenRTB (Real-Time Bidding). IAB—Empowering the Marketing and Media Industries to Thrive in the Digital Economy*. Accessed: Jan. 8, 2018. [Online]. Available: https://www.iab.com/guidelines/real-time-bidding-rtb-project/
[40] Google. Latency Restrictions and Peering | Real-Time Bidding Protocol. Google Developers. Accessed: Jan. 8, 2018. [Online]. Available: https://developers.google.com/ad-exchange/rtb/peer-guide
[41] J. M. Drange. *Markedsførere Krever Omfattende Reform AV Det Digitale Annonsesystemet*. Accessed: Jun. 1, 2018. [Online]. Available: https://www.anfo.no/markedsforere-krever-omfattende-reform-av-det-digitale-annonsesystemet
[42] C. Nyst, "Children and digital marketing—Rights risks and responsibilities," UNICEF, Geneva, Switzerland, Tech. Rep., Apr. 2018. [Online]. Available: https://www.unicef.org/csr/css/Children_and_Digital_Marketing_-_Rights_Risks_and_Responsibilities.pdf
[43] M. Marciel *et al.*, "Understanding the detection of view fraud in video content portals," in *Proc. 25th Int. Conf. World Wide Web*, Montreal, QC, Canada, 2016, pp. 357–368.
[44] A. Badhe, "Click fraud detection in mobile ads served in programmatic exchanges," *Int. J. Sci. Technol. Res.*, vol. 5, no. 4, p. 1, Apr. 2016.
[45] M. Kotila, "WFA guide to programmatic media (what every advertiser should know about media markets)," World Fed. Advertisers, Brussels, Belgium, Tech. Rep., 2014.
[46] P. Callejo, R. Cuevas, A. Cuevas, and M. Kotila, "Independent auditing of online display advertising campaigns," in *Proc. 15th ACM Workshop Hot Topics Netw.*, Atlanta, GA, USA, 2016, pp. 120–126.
[47] *Production Transparency in the U.S Advertising Industry*, Assoc. Nat. Advertisers, New York, NY, USA, 2017.
[48] J. Yli-Huumo, D. Ko, S. Choi, S. Park, and K. Smolander, "Where is current research on blockchain technology?—A systematic review," *PLoS ONE*, vol. 11, no. 10, p. e0163477, Oct. 2016.
[49] B. Walsh. (Aug. 14, 2013). *The Surprisingly Large Energy Footprint of the Digital Economy*. [Online]. Available: http://TIME.com
[50] Digiconomist. *Ethereum Energy Consumption Index (Beta)*. Accessed: Jun. 1, 2018. [Online]. Available: https://digiconomist.net/ethereum-energy-consumption
[51] A. Jacobson, "Method of block chain verification to authenticate advertising payment chains," Technical Disclosure Commons, Berkeley, CA, USA, Tech. Rep., Mar. 2017.
[52] adChain. *adChain—Unlocking the Blockchain for Digital Advertising*. Accessed: Jan. 8, 2018. [Online]. Available: https://d2x21ttkvtoazg.cloudfront.net/
[53] AdEx. *What is AdEx*. Accessed: Jan. 8, 2018. [Online]. Available: http://adex.network/
[54] R. Kastelein. (Jun. 22, 2017). Comcast's Advanced Advertising Group and Participants Announce Blockchain-based Technology Platform. BlockchainNews. Accessed: Jan. 8, 2018. [Online]. Available: http://www.the-blockchain.com/2017/06/22/comcasts-advanced-advertising-group-participants-announce-blockchain-based-technology-platform/
[55] L. O'Reilly. (Apr. 7, 2016). 'BLATANTLY ILLEGAL': 17 Newspapers Slam Ex-Mozilla CEO's New Ad-Blocking Browser. Business Insider. [Online]. Available: http://www.businessinsider.com/newspaper-publishers-send-cease-and-desist-to-brave-browser-2016-4?r=US&IR=T&IR=T
[56] R. McMillan. (Mar. 3, 2014). The Inside Story of Mt. Gox, Bitcoin's $460 Million Disaster | WIRED. Wired. Accessed: Jan. 23, 2018. [Online]. Available: https://www.wired.com/2014/03/bitcoin-exchange/
[57] Quartz. *Crypto-Crisis: Everything You Need to Know About the Ethereum 'Hard Fork'* Accessed: Aug. 1, 2018. [Online]. Available: https://qz.com/730004/everything-you-need-to-know-about-the-ethereum-hard-fork/
[58] J. Buntinx. (May 26, 2017). Coinbase Issues Make it More Difficult to Sustain Bitcoin Bull Run. NewsBTC. Accessed: Jan. 8, 2018. [Online]. Available: http://www.newsbtc.com/2017/05/26/coinbase-issues-make-difficult-sustain-bitcoin-bull-run/
[59] *Nyiax*. Accessed: Jan. 8, 2018. [Online]. Available: https://www.nyiax.com/
[60] Coinmarketcap. *Cryptocurrency Market Capitalizations*. Accessed: Jan. 8, 2018. [Online]. Available: https://coinmarketcap.com/currencies/adtoken/
[61] Thomas Fox-Brewster's. (Dec. 20, 2016). Biggest Ad Fraud Ever': Hackers Make $5M A Day by Faking 300M Video Views. Forbes. Accessed: Jan. 8, 2018. [Online]. Available: https://www.forbes.com/sites/thomasbrewster/2016/12/20/methbot-biggest-ad-fraud-busted/#11f12ff84899
[62] Steemit. (Jul. 26, 2016). *How Agile is your Chain?—Top Digital Currencies—Transaction Per Second Comparison*. Accessed: Jan. 8, 2018. [Online]. Available: https://steemit.com/steem/@steempower/how-agile-is-your-chain-top-digital-currencies-transaction-per-second-comparison
[63] Steemit. (May 31, 2017). *Ethereum Downtime—Possible Issue (Breaking)*. Accessed: Jan. 8, 2018. [Online]. Available: https://steemit.com/ethereum/coinlord/ethereum-downtime-possible-issue-breaking
[64] Ethereum. *Ethereum Project*. Accessed: Jan. 8, 2018. [Online]. Available: https://www.ethereum.org/

[65] Ripple. *Join RippleNet*. Accessed: Jan. 8, 2018. [Online]. Available: https://ripple.com/
[66] Counterparty. *Protocol Specification | Counterparty*. Accessed: Jan. 8, 2018. [Online]. Available: https://counterparty.io/docs/protocol_specification/
[67] *Omni Layer*. Accessed: Jan. 8, 2018. [Online]. Available: http://www.omnilayer.org/
[68] E. Kokoris-Kogias, P. Jovanovic, L. Gasser, N. Gailly, E. Syta, and B. Ford, "OmniLedger: A secure, scale-out, decentralized ledger via sharding," in *Proc. IEEE Symp. Secur. Privacy (SP)*, May 2017, pp. 583–598.
[69] C. Odom. *Open-Transactions: Secure Contracts Between Untrusted Parties*. [Online]. Available: http://www.opentransactions.org/open-transactions.pdf
[70] BitShares. *BitShares—Your Share in the Decentralized Exchange*. Accessed: Jan. 8, 2018. [Online]. Available: https://bitshares.org/
[71] BitShares. *Industrial Performance and Scalability*. Accessed: Jan. 8, 2018. [Online]. Available: https://bitshares.org/technology/industrial-performance-and-scalability/
[72] B. Wiki. *Colored Coins*. Accessed: Jan. 8, 2018. [Online]. Available: https://en.bitcoin.it/wiki/Colored_Coins
[73] *Lightning Network*. Accessed: Jan. 8, 2018. [Online]. Available: https://lightning.network/
[74] O. Mishli. (Jan. 26, 2017). Key Protection and Key Governance in Blockchain. Dyadic. [Online]. Available: https://www.dyadicsec.com/key-protection-and-key-governance-in-blockchain/
[75] Nameles. *Open Source Invalid Traffic Detection*. Accessed: Jan. 8, 2018. [Online]. Available: http://nameles.org/

MATTI PÄRSSINEN received the M.Sc. and MBA degrees in 2016 and 2008, respectively. He is a currently a Researcher with the Department of Communications and Networking, Aalto University. The focus of his research is on ICT energy efficiency. He has over 20 years of experience in the field of telecommunications and ICT, pioneering in 2.5G and 3G global deployments. He has comprehensive knowledge of mobile operator technologies, business, and strategy in the fields of cellular networks, network security, connectivity, and data centers.

MIKKO KOTILA started one of the first digital agencies and is an Innovator and a Researcher in the Online Advertising Ecosystem. He has authored *WFA's Guide to Programmatic Media*, *WFA's Compendium of Ad Fraud Knowledge*, and multiple scientific research papers focused on online advertising. In 2014, he has co-founded and chaired I-COM's Data Science Board, and co-founded I-COM's Blockchain Committee. He is an Adviser for the World Federation of Advertisers and various national advertiser associations. He is the Principal of Botlab, the only non-profit foundation with a focus on blockchain research in the online advertising context.

RUBÉN CUEVAS RUMIN was born in Madrid, Spain, in 1981. He received the Ph.D. and M.Sc. degrees in telematics engineering, and the M.Sc. degree in telecommunications engineering from the University Carlos III of Madrid, Spain, in 2010, 2007, and 2005, respectively, and the M.Sc. degree in network planning and management from Aalborg University, Denmark, in 2006. Since 2006, he has been a member of the Telematic Engineering Department and the NETCOM Research Group, where he is currently an Assistant Professor. In 2012, he was a Courtesy Assistant Professor with the Computer and Information Science Department, University of Oregon. From 2008 to 2009, he was an Intern at the Internet Scientific Group, Telefonica Research Lab Barcelona.

He has co-authored over 70 papers in prestigious international journals and conferences such as the ACM CoNEXT, WWW, ACM HotNets, IEEE Infocom, ACM CHI, IEEE/ACM TON, IEEE TPDS, and PlosONE or Communications of the ACM. He has been the PI of nine research projects funded by the EU H2020 and FP7 programs, the national government of Spain and private companies. He has participated in over 15 research projects. His main research interests include online advertising, web transparency, personalization and privacy, online social networks, and internet measurements.

AMIT PHANSALKAR has completed his graduate work at Los Alamos National Labs. He has four patents and over 20 peer-reviewed publications. He started his career in systems biology, building protein interaction systems in the human proteome. He has co-founded Cognika, a cognitive computing platform. He has also served in a variety of industry roles, including the Global Head of data sciences for Kantar and the Chief Data Officer for Massmutual, a Fortune 100 financial services company. He also co-founded Netra Systems, a machine vision company. He was the Founding Chair of the I-COM Data Science board and currently serves on the Board of Botlab.

JUKKA MANNER was born in 1972. He received the M.Sc. and Ph.D. degrees in computer science from the University of Helsinki in 1999 and 2004, respectively. He is currently a Full Professor (tenured) of networking technology with the Department of Communications and Networking (Comnet), Aalto University. He has authored over 100 publications, including 11 IETF RFCs. His research and teaching focuses on networking, software, and distributed systems, with a strong focus on wireless and mobile networks, transport protocols, energy-efficient ICT, and cyber security. He has been the Principal Investigator and the Project Manager for over 15 national and international research projects. From 2008 to 2012, he was the Academic Coordinator for the Finnish Future Internet Research Program. He is an active Peer Reviewer and a member of various TPCs. In 2014, he received the Cross of Merit, Signals, and the Medal for Military Merits for contributions in national defense and C4 in 2015. He was the local Co-Chair of Sigcomm 2012, Helsinki. He has contributed to the standardization of Internet technologies in the IETF since 1999, and was the Co-Chair of the NSIS Working Group.