Blockchain in Ad Tech

November 2017

acxiom Research

RECOMMENDATIONS

- **Blockchain will be a real game changer.** Blockchain is an outcome of the on-going economic, social, and technical trends that have driven the Web's evolution to this point. The information economy is very efficient at driving down the marginal cost of production of goods and services. The next significant disruption will be to the business models of trusted third parties whose services cause production costs to exceed the marginal costs available through the new combination of technologies like peer-to-peer, cryptography, consensus algorithms based on game theory, and self-sovereign identity – i.e., blockchain.

- **But the horizon for the impact of disruptive change is three – five years.** Blockchain networks are not yet scalable or secure enough for production deployments by enterprises. Ethereum can currently process on average about 100 transactions/minute, nowhere near the scale or speed needed for manipulating large databases or millions of real-time programmatic transactions. Several technologies that may allow blockchain-based networks to scale in the millions of transactions/minute, like Plasma, Raiden, and Sawtooth, are in early development. Any significant tests of scalability are at least twelve months away, and then it will take substantial time after scalability is proven to pass these platforms through the numerous security reviews necessary to prove them ready to handle enterprise-grade applications.

- **Ignore today's madness of crowds and ICO speculative bubble – most of these companies will not survive.** However, there are high-value use cases in Blockchain 1.0 driven by real economic trends and business models. In marketing and advertising, these use cases include anonymous identity management, simplification of the ad tech value chain, simple, easily reconciled accounting for online advertising campaigns, reduction of ad fraud, taxonomy management, content and content rights management, and next-generation privacy. 2018 should yield some initial forays utilizing blockchain tech, even as there is less talk about blockchain being the magical pixie dust that can just be sprinkled atop everything[1].

- **To do blockchain you must first change your thinking to a framework where trust is an unknown commodity, everybody is potentially a very shrewd bad actor, and where security and accurate recording of a transaction must be achieved without a trusted third party.** Read books on game theory. Train yourself to think like a security expert fighting network threats. There is always someone else with a new algorithm trying to hack the network. In blockchain terms, that means being able to change the ledger so that a fraudulent transaction is perceived as true by the majority of the nodes on the network, known as a false consensus.

[1] George Howard. "What is Blockchain Technology? A Step-by-Step Guide for Beginners" (Blockgeeks, https://blockgeeks.com/guides/what-is-blockchain-technology/)

- **Ask "Why Blockchain?"** Blockchain 1.0 feels a lot like Web 1.0 in its infancy. At the beginning of Web 1.0, many companies began by moving their traditional business onto the platform and attempting to operate using the same or similar business models. Right now, many enterprises new to blockchain are taking that same approach. The result is that blockchain does not look attractive because it is nowhere near cost effective versus existing technologies for current business models. With any new proposal, ask whether blockchain provides unique advantages. If the approach seems very similar to how you approach the problem today, it probably isn't making use of the fundamental power of the technology.

- **Pay Attention to Use Cases Based on the Clayton Christianson's Disruption Model.** In The Innovator's Dilemma, Clayton Christian described the method by which new technologies disrupt an existing business model: they are less functional but less expensive, the existing competitor can't lower costs enough to compete at that price point and it leaves a "price umbrella" under which the new competitor can survive and grow. Look for use cases that fit this model. An example of two approaches is ads.txt vs. AdChain's solution for ad fraud. AdChain can succeed because the hidden costs of the ads.txt standard (manual updating of servers, exposing publisher relationships) makes it costlier than what a blockchain-based solution can deliver.

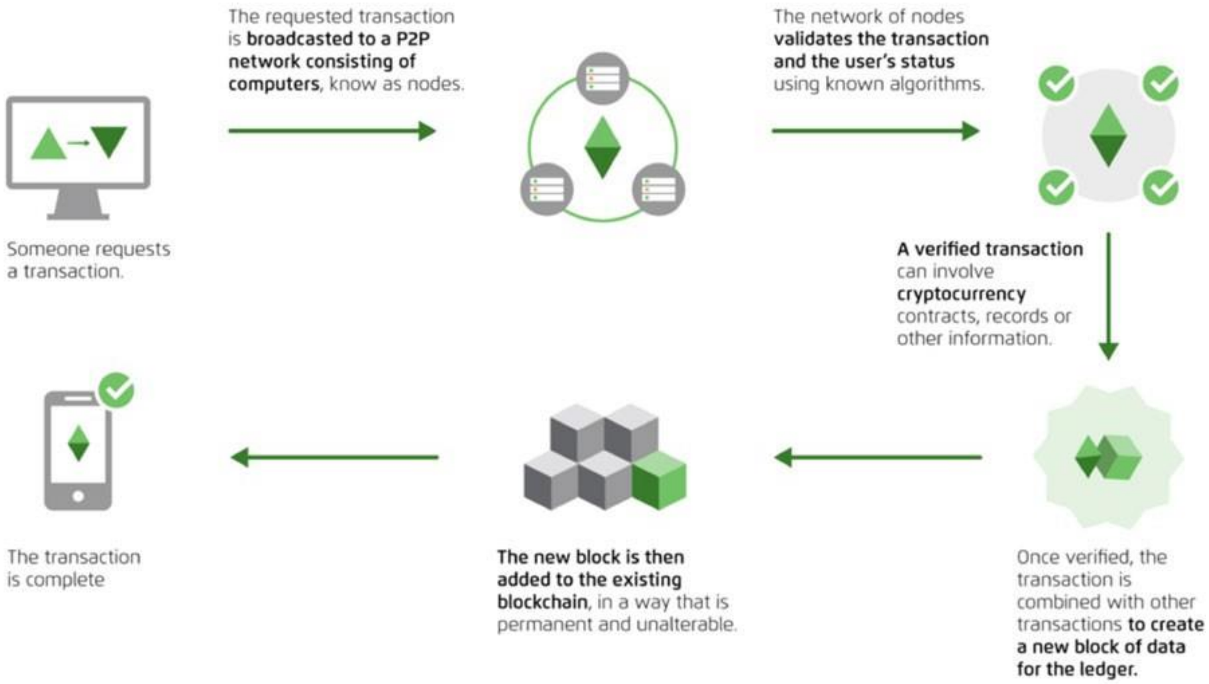
INTRODUCTION

Blockchain has become the hottest new technology on the planet. Everywhere you look, there is another article boldly claiming that blockchain is "as big as the Internet" or that it is "going to change doing business as we know it." Blockchain does have huge promise, both generally and for ad tech specifically. But at this moment, it is just that – a promise. The paper explores some unique aspects of blockchain's promise that make it such an interesting new technology for ad tech. We look at its conceptual underpinnings, the state of the technology, the economic implications, and the areas which provide the most likely use cases for early blockchain applications.

WHAT IS BLOCKCHAIN?

In its simplest form, blockchain is a network of distributed ledgers with no central authority and a mechanic like that shown in Figure 1. In a blockchain network, each transaction is a block that contains all the information about all the prior blocks thus forming a "block chain" which is permanent, practically impervious to tampering, and thus trustworthy for recording what are known as "smart contracts."

Figure 1 - Basic Conceptual Flows in Blockchain


The requested transaction is **broadcasted to a P2P network consisting of computers**, know as nodes.
The network of nodes **validates the transaction and the user's status** using known algorithms.
Someone requests a transaction.
A verified transaction can involve **cryptocurrency** contracts, records or other information.
The transaction is complete
The new block is then added to the existing blockchain, in a way that is permanent and unalterable.
Once verified, the transaction is combined with other transactions **to create a new block of data for the ledger.**

Source: PWC "A Primer on Blockchain"

While that description is good as far as it goes, it does not explain what blockchain really is and why it is so difficult to create a mental model upon which to design new products or services.

Blockchain is best described as a combination of game theory, cryptographic algorithms, and peer-to-peer networking, with a dash of libertarian[2] political thinking mixed in to make things interesting. There are six core assumptions you need to internalize to "get your head around" blockchain:

1. Blockchain assumes a large, distributed, digital community participating in economic activity between peers on the edge of the network (a peer-to-peer network), whether it is electronic money movement, documentation of physical contracts, validating someone's identity, or sales of goods that require an immutable record of the transaction – in other words, a historic accounting ledger.

2. There are untrusted individuals in the community who, given the opportunity, will cheat. However, no one on the network knows who is and is not trustworthy. Thus, the assumption is no one is.

   Cheating, in this case, means changing the ledger to the detriment of one or more honest community members. That could mean undoing a payment entry so the cheater doesn't owe money or, alternatively, changing contract terms to pay them for a service never delivered.

   It could also mean, to give a specific example involving no exchange of monetary value, that the cheater posts a "fake news" story to Facebook and then alters the ledger on a "news certification blockchain" to show that it was certified as "real news."

[2] Many would say anarchist.

3. Everyone in the network wants their own copy of the ledger that is updated with every new transaction from anyone on the network, and wants everyone else to have one as well. This provides “truth through consensus.” The true transaction is one where the majority of ledgers agree it occurred as entered. Tampering with one ledger among hundreds will not change the consensus.

4. No third-party organization can be trusted as a regulator/ombudsman for the network. Since they sit outside the blockchain (otherwise they can’t act as ombudsman), they may have other rational incentives to manipulate the system. Thus, no economic justification exists to pay a third party to assume risk. The network must work without trusted third-parties like banks or escrow companies.[3]

5. Everyone on the network is incredibly ingenious (and/or has access to very smart AI tools). So that when a mechanic, such as a consensus algorithm, is deployed to preserve the integrity of the ledger from tampering, it is assumed that the bad actors on the network will try to circumvent it.

6. Everyone in the network is a rational economic actor.[4] Thus, cheating within the community will not occur If the cost of that behavior significantly higher than the gains from cheating.[5] This is a crucial role tokens play on a blockchain network. They put a cost to both the gain (in the case of the Facebook example, having a news post certified as true) and to cheating. This is why blockchain networks that solve problems having nothing to do with money still issue coins.

Note that these assumptions say nothing about speed, performance, or scalability of the network. Nor is there any mention of encryption or other enabling technologies. In fact, other than the assumption of an existing Internet (or its private equivalent) there are no technical assumptions anywhere because blockchain isn’t about technology, it is about psychology. To be specific, the psychology of gamers playing “Spy vs. Spy” on a massive online multiplayer role-playing game where the game and its rules are determined by:

- the purpose of the blockchain network
- the type of value exchanges it supports
- the rules that have been established and are maintained only by algorithms built into the network.

The bad guys, whose identities are unknown and constantly changing, are always trying to cheat. The good guys are always trying to anticipate the next attack and devise updated algorithms to protect the network’s integrity. That is why you must first understand game theory if you wish to understand how blockchain can help your business.

[3] And if you can build a system that doesn’t need a trusted third party, then why pay for that service? In other words, blockchain technology creates a virtuous cycle where solving for one goal (removing untrusted institutions) achieves an economic goal of reducing marginal costs of transactions making the untrusted institution economically unnecessary.

[4] There are discussions today in Ethereum about how to make the network work if you assume that not all actors are economically rational. As an example, a terrorist may not care if it costs a lot if he is discovered doing something illegal because his political goals far outweigh any costs associated with cheating.

[5] One of the on-going discussions in any blockchain is how high the cost of cheating should be relative to the gain to deter cheating.

BLOCKCHAIN AND GAME THEORY

Game theory considers how players of a mathematically formalized game who cannot communicate can and will (being rational) optimize their decisions. The issue is that one person's decision influences others in the group. Game theory predicts the best choice participants will make toward achieving a specific goal in the situation of interdependent decision-making. In other words, it is about the psychology of individuals and how they will act in a closed system where:

- other individuals are also trying to achieve the same goal
- there are a specific set of incentives applicable to all the individuals (players in the game).

Thomas Schelling, the Nobel Prize winner in game theory described the final result or "equilibrium" in such a system in the absence of communication as being based on "each person's expectation of what the other expects him to expect to be expected to do." [6]

A simple game theory example many people have been exposed to is The Prisoner's Dilemma. Appendix A provides a more sophisticated example that provides a window into the mindset blockchain designers bring to their work. First, they make assumptions about the psychology of actors (both good and bad) in the system, they model it with a game-theoretical scenario, and then they design incentives to ensure the desired interdependent decision-making.

Bitcoin and Ethereum, the two largest blockchain networks, depend on two critical game theoretical challenges/ solutions. The first is called the Byzantine General's Problem. The second is known as Proof of Work or, on Ethereum in an upcoming release, Proof of Stake. The latter two are examples of consensus algorithms used to overcome the Byzantine General's Problem. And while The Byzantine General's Problem was a concept that arose from computer and P2P networks[7], Proof of Work was Satoshi Nakamoto's unique addition that made Bitcoin, and blockchain generally, feasible.

The Byzantine General's Problem (BGP) was first formulated in 1982 by Leslie Lamport, Robert Shostak, and Marshall Pease at SRI.[8] It was designed to solve a computer network reliability problem where one or more malfunctioning components are sending faulty ("traitorous") messages to the rest of the network's components. It is important to blockchain because of blockchain's distributed ledger and the need for all the ledgers to agree. The basic notion of the BGP can be summarized as follows:

> *A Byzantine army has surrounded and set siege to a castle. The generals, physically separated and commanding different units of the army, realize that that they need to decide on a coordinated attack or coordinated retreat. It is important that the majority commits to one or the other, as a mistimed or half-hearted*

[6] Schelling, Thomas C. The Strategy of Conflict (First ed.). (Cambridge: Harvard University Press, 1960), page 57. Also, these equilibria or "focal" points for a solution are known as Schelling Points, in honor of their inventor. You will often see this term in blockchain articles.

[7] Fedotova, Natalya and Veltri, Luca. "Byzantine Generals Problem in the Light of P2P Computing." Presented at IEEE Conference on Mobile and Ubiquitous Systems, July 17-21, 2006.

[8] Lamport, Leslie and Shostak, Robert and Pease, Marshall. "The Byzantine Generals' Problem." (Menlo Park: SRI international, 1982). Published in ACM Transactions on Programming Languages and Systems, Volume 3, Number 4, July 1982, pages 382-401.

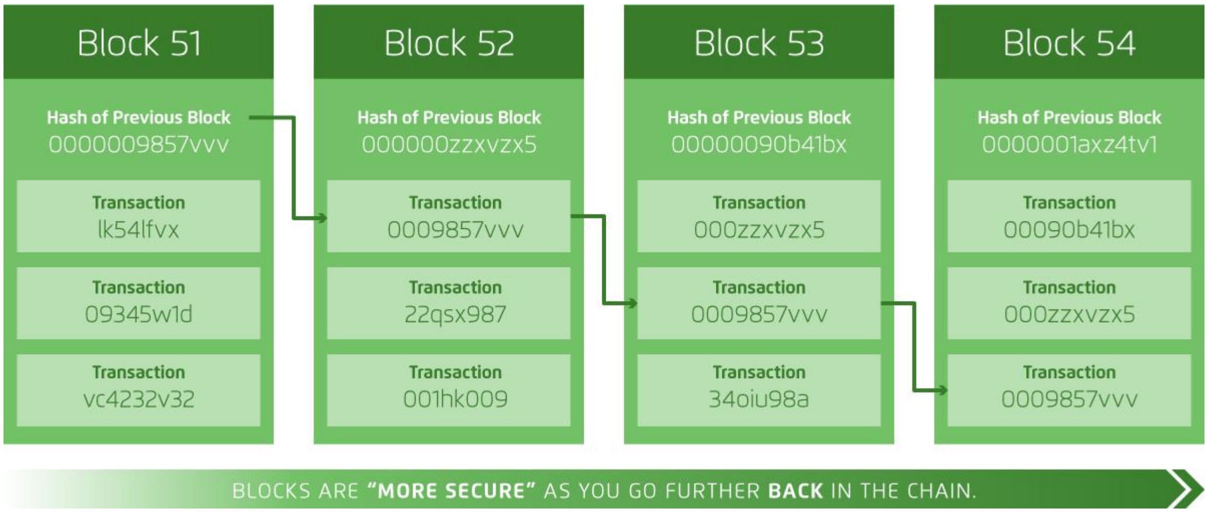
attack would mean major losses and a far worse outcome for the Byzantines. Unfortunately, there are an unknown number of traitorous generals in the Byzantine ranks who would like the campaign to end disastrously. They may send conflicting messages to different generals hoping to sabotage the effort. Furthermore, since messages must be relayed by messenger, it is also impossible to tell if these messages are forged or authentic.

The central question is this: in a system where consensus is necessary, how can a unanimous agreement be reached by good processes in the absence of trust? In other words, how can these generals overcome the traitors within and reach a coordinated, majority decision?

The solution that Nakamoto created used a pricing model, called Proof of Work, where computer processing time stands in for money, since each unit of computer processing time has an associated monetary cost. This allowed his design to meet the criteria of assumption 6. Bitcoin assures the integrity of its ledger by making any attempt to change the ledgers across the network so astronomically expensive as to be not worth trying.

Proof of Work forces each server containing a ledger to solve a very difficult mathematical problem and distribute instantaneously the solution (with the transaction) to all the other servers. That problem is difficult enough to use a significant amount of computer processing time. Once the block is sent to all the other servers, each of them must add a new transaction to the prior block and compute another solution to the problem. Whoever finishes fastest publishes to all the other servers. The other servers then append a transaction to the block and do the same over and over. As each block is added to the chain, the cost of altering a transaction further back across all servers becomes exponentially more expensive with each round. It quickly becomes astronomical, and thus the historic ledgers are safe from tampering.

Figure 2- How Proof of Work Enables the Blockchain



Source: Toptal, "Blockchain Technology Explained"

Proof of Stake (PoS) is an alternate way of solving the requirement of assumption 6. It is of interest because the processing costs, energy use, and time required to solve the mathematical problem in Proof of Work will not scale to other types of problems blockchain can uniquely solve. PoS is a deterministic mechanism for protecting the ledgers in blockchain that uses the actual cryptocurrency of the network to assign a "validating server" to a transaction. With PoS, you do not solve any cryptographic puzzle. Instead, the validator is given the right to create a single block, which must also point to the prior block. The right is based on the validator paying for the privilege to validate. That is to say, they place a bet – stake money – to get a seat at the table.

Any node that holds the blockchain's base cryptocurrency (in Ethereum's case, ether) becomes a validator by sending a special type of transaction that locks up their coins into a deposit. The likelihood of being assigned a validation task is directly proportional to the number of coins deposited by the validator, so someone who deposits 200 coins is twice as likely to be assigned as a validator with 100 coins. Once assigned, the validator has a certain period to process the block, or else it is assigned to another validator and the original validator loses a small portion of their stake. So, there is good reason for a validator to ensure their underlying infrastructure performs. And if a validator breaks the rules by trying to commit two different blocks at the same time, for example, they stand to lose their entire stake.

Both these methods are about encouraging or discouraging specific behaviors among individuals who do not know, and therefore do not trust, each other. Each method – and there are approximately 20 others being tested – has its strengths and weaknesses[9]. As Vitalik Buterin the founder of Ethereum wrote:

> *"Every approach to behavior, to consensus, whether it be Nakamoto consensus, social consensus, shareholder voting consensus, leads to its own set of conclusions and leads to a system of values that makes quite a bit of sense when viewed on its own terms—though they can certainly be criticized when compared against each other."*[10]

The important question that such a system poses is whether consensus algorithms - the game-theoretical models underlying any blockchain, public or private – can ever be designed strongly enough to convince enterprises to transact trillions of dollars on the technology. Can they be made secure enough against an attack by a dogged cheater? In general, the answer is yes. However, it does not mean that production-grade blockchain-based solutions will be available in large quantity any time soon.

Not only do consensus algorithms need time for robust testing, but the scalability of existing blockchain platforms is insufficient to handle a broad range of use cases. The current design of the major blockchain platforms trades off computational efficiency and scale for transactional integrity. Today Bitcoin can process 2-3 transactions per second; Ethereum about 20.[11] Visa and Mastercard process about 10,000 transactions per second, and a reasonably-sized ad network like AdMob can generate approximately 1,500 requests per second. Ethereum has been working on solutions, such as the Raiden Network and Truebit. Vitalik Buterin and Joseph Poon announced in August the Plasma Project, based on Lightning. Hyperledger Fabric, the

[9] Proof of Stake has its detractors as well. See "The Inevitable Failure of Proof-of-Stake Blockchains and Why a New Algorithm is Needed." The Coin Telegraph, May 24, 2015. https://cointelegraph.com/news/the-inevitable-failure-of-proof-of-stake-blockchains-and-why-a-new-algorithm-is-needed) and McElrath, Bob. "What's Wrong with Proof of Stake." The SolidX Blog, June 14, 2016. https://blog.sldx.com/whats-wrong-with-proof-of-stake-77d4f370be15.

[10] Buterin, Vitalik. "A Proof of Stake Design Philosophy." Medium, December 30, 2016. https://medium.com/@VitalikButerin/a-proof-of-stake-design-philosophy-506585978d51

[11] "Bitcoin and Ethereum vs Visa and PayPal – Transactions per second" Altcointoday, April 22, 2017). http://www.altcointoday.com/bitcoin-ethereum-vs-visa-paypal-transactions-per-second/

blockchain platform developed by the Apache Foundation, is designed for 100,000 transactions per second. But none of these are deployed and no clear date when they will be ready, working and proven robust. Large enterprises will want confidence in the technology before they deploy production-scale systems into the marketplace. This will be especially true for those dealing with sensitive financial or PII-based information. The type of hesitancy will probably be similar to what cloud providers experienced when convincing enterprise customers to move sensitive information into cloud-based platforms like AWS. Given these issues, production-scale blockchains are likely 2-3 years into the future, especially in ad tech.

BLOCKCHAIN AND THE ECONOMICS OF AD TECH

What is Cryptoeconomics?

Cryptoeconomics is a formal discipline that studies how blockchain networks and their protocols impact the production, distribution and consumption of goods and services in a decentralized digital economy. This study is less than six months old, and there are only a handful of people who have been working in the field. Yet it can provide a framework to understand how blockchain and its associated technologies will impact ad tech over the next few years.

As it has emerged over more than 150 years, the networked information economy has driven out any cost from economic value chains that is above the marginal cost of production available through the combination of the decreasing costs of communication, computing, and storage.[12] We have seen this accelerate through two phases of the Worldwide Web. Web 1.0 drove out costs of physical distribution of media, such as newspapers, books, music and video, that could be distributed digitally through the network at almost zero marginal cost per unit. Web 2.0 most impacted the marketing, sale and distribution of physical goods. Companies whose business was centered on moving goods from sellers to buyers found themselves disintermediated as manufacturers could present their products to consumers online and deliver goods directly to them via global overnight delivery networks. Retailers dependent on physical footprints also found themselves in decline as the marginal cost of presenting goods to buyers declined. Television and print advertising, as well as direct mail shrank as advertisers benefited from lower costs and better measurement available via email, paid search, and online display.

Yet both these phases had one thing in common: the need for centralized, trusted third parties to mitigate financial and other risks, as well as act as safe havens for sharing sensitive personal or business data. These were often extensions of existing business models from the pre-digital economy, although not always. Before credit card companies found a way to extend their payment networks online, PayPal evolved to mitigate payment and delivery risks. RSA, Verisign, DigiCert and others evolved to mitigate identity risk (through digital signatures) and assure communication integrity (via encryption). Government extended its role as a trusted third party for privacy from direct mail and phone into the digital space. As email spam and other issues arose, governments mandated features on web sites like clearly available opt outs and easy-to-find (if not to read) privacy policies with serious fines for companies caught failing to comply.

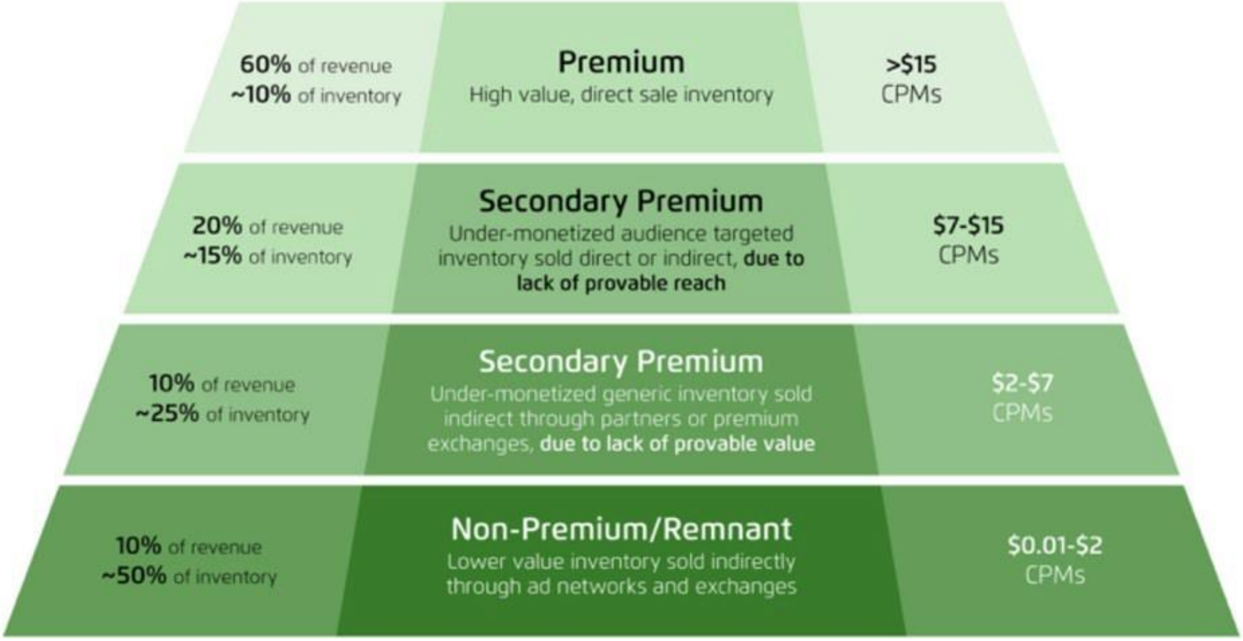
[12] See Yochai Benkler's classic tome The Wealth of Networks: How Social Production Transforms Markets and Freedom (New Haven: Yale University Press, 2006) for an insightful in-depth study into this arena.

Web 3.0, as it is coming to be known, will disrupt the business of these trusted third parties as the continuing evolution of technology drives down the marginal costs of “ensuring trust” via technologies like blockchain that allow for secure and private peer-to-peer commerce. A very early example of this peer-to-peer production was the development of consumers as a distributed “trusted third party” for ensuring product and service quality. Good consumer reviews in multi-merchant marketplaces like Amazon or shopping.com drive increased sales. Companies now watch social media continuously for bad buzz about some customer service brouhaha and will react almost instantaneously to fix it. Today Bitcoin and other cryptocurrencies work for peer-to-peer transactions without a central bank to issue currency, a credit card issuer to provide credit, or a payment processer to process transactions and perform settlement. This is just the beginning for online commerce, and ad tech as a purely online ecosystem will be as impacted by these trends as much as any industry.

PROGRAMMATIC ADVERTISING ECONOMICS MEETS CRYPTOECONOMICS

Figure 3 represents how publishers generate revenue from digital display advertising. Generally – and these are averages that can vary from publisher to publisher - direct sales of premium display to advertisers, which represent only 10% of their inventory, generate 60% of revenue. The bottom of the pyramid represents pure programmatic inventory sales, which represent approximately 50% of inventory and only 10% of revenue. In the middle are two layers, together representing about 40% of inventory. The first is non-programmatic, indirect sales of premium inventory, which generate on the order of 20% of revenue. The second is programmatic premium inventory, which represents about 10% of revenue.

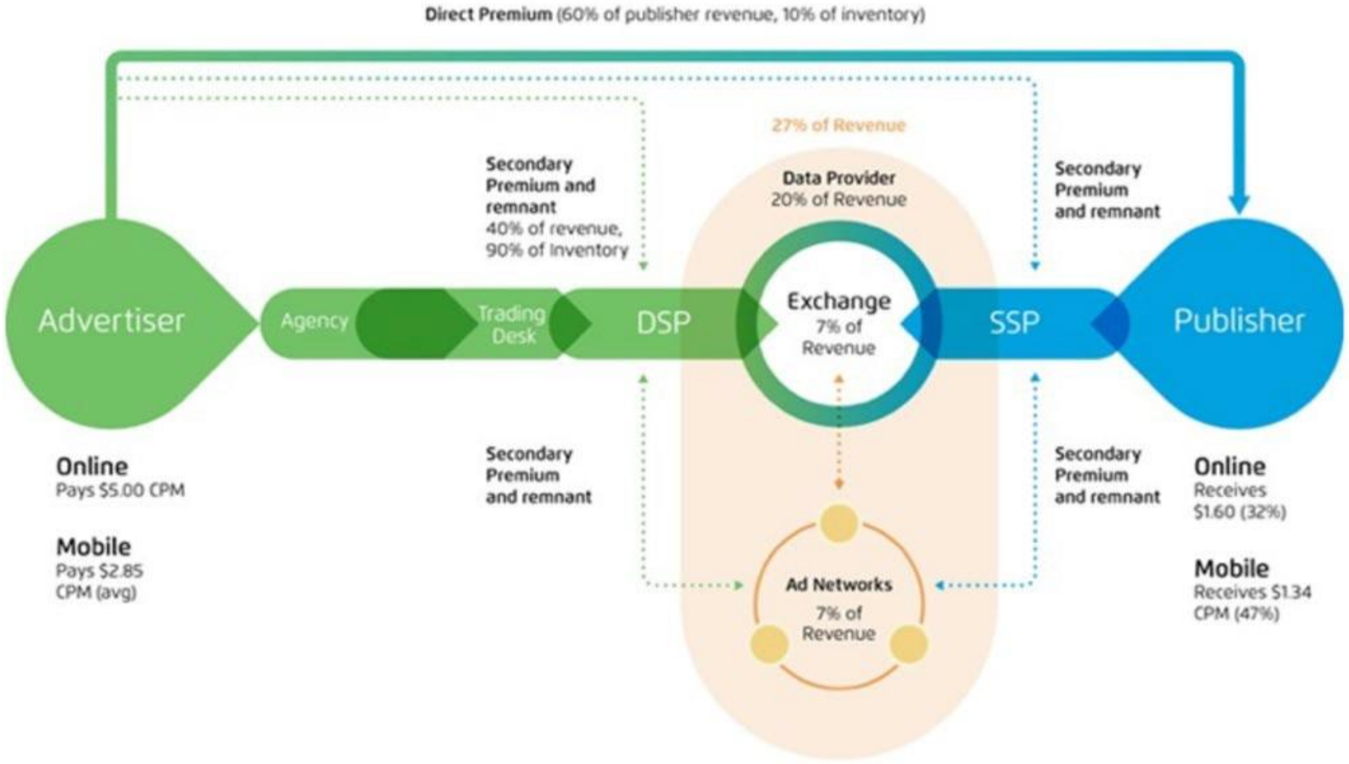
Figure 3 - The Economic Pyramid of Online Publisher Revenue from Digital Display Advertising


60% of revenue
~10% of inventory
Premium
High value, direct sale inventory
>$15
CPMs
20% of revenue
~15% of inventory
Secondary Premium
Under-monetized audience targeted inventory sold direct or indirect, due to lack of provable reach
$7-$15
CPMs
10% of revenue
~25% of inventory
Secondary Premium
Under-monetized generic inventory sold indirect through partners or premium exchanges, due to lack of provable value
$2-$7
CPMs
10% of revenue
~50% of inventory
Non-Premium/Remnant
Lower value inventory sold indirectly through ad networks and exchanges
$0.01-$2
CPMs

Source: Internal, developed from conversations with ad tech participants

Figure 4 represents the value chain in programmatic display advertising. It also shows the percentage of revenue taken by each layer. What has always been fascinating about this diagram is the number of stages in the value chain, how “blurred” these stages tend to be, and the cost structure.

Figure 4 - The Programmatic Advertising Value Chain


Direct Premium (60% of publisher revenue, 10% of inventory)
27% of Revenue
Secondary Premium and remnant 40% of revenue, 90% of inventory
Data Provider 20% of Revenue
Secondary Premium and remnant
Advertiser
Agency
Trading Desk
DSP
Exchange 7% of Revenue
SSP
Publisher
Online Pays $5.00 CPM
Mobile Pays $2.85 CPM (avg)
Secondary Premium and remnant
Secondary Premium and remnant
Ad Networks 7% of Revenue
Online Receives $1.60 (32%)
Mobile Receives $1.34 CPM (47%)

Source: Internal, developed from discussions with ad tech participants

There are several challenges for advertisers and publishers implicit in these diagrams for which blockchain may offer a unique solution.

1. The Publisher Pays a Great Deal to Generate 20% of Revenue. Programmatic display inventory represents approximately 20% of publishers' revenue. But for every dollar spent in programmatic by advertisers, publishers only ultimately receive about 35%. The other 65% is consumed by the players in a very fragmented, tangled, and inefficient value chain of several hundred companies.[13] Publishers are unlikely to increase prices for the bottom 50% of impressions, as they represent remnant inventory that will continue to exist in a world of 15% fill rates. The only way to improve profitability of this layer is to lower delivery costs. This means finding more ways to go direct from advertiser to publisher, disrupting the business models of companies in between.

   How might blockchain disrupt the business model of a DSP, for example? A DSP adds value in multiple ways. However, its fundamental value proposition is to allow a single advertiser to reach the same audience across multiple touchpoints by optimally submitting bids across multiple ad networks and

[13] This includes agencies, trading desks, DSPs, exchanges, ad networks, DMPs, and SSPs across both the online and mobile ecosystems. Exactly how this number is calculated varies from company to company, but you can just quickly count the number of logos on both the Display and Mobile Lumascape diagrams to get a sense of scale (https://www.lumapartners.com/luma-content/).

publishers. This involves submitting millions of ad requests and receiving millions of responses across hundreds of networks. Now imagine a blockchain (peer-to-peer) based model, where an advertiser makes a single request for an audience to the blockchain which immediately propagates to all publishers on the network. The blockchain network itself has algorithms built in that take the request and responses on the chain, look for the optimal spend (since each member of an audience has a single identity across all publishers), and then submit the order directly to the publishers. Conceptually, this approach would have a similar disruptive impact on SSP business models. DSPs, SSPs, or other players would become operators of the blockchain network or provide value-added services on or to the blockchain. A model like this could reduce costs to the publisher and/or reduce the number of participants in the value chain.

2. Connecting Consumers' Identity and their Data. Every provider in the programmatic value chain has a unique identifier for their customer, and rarely do these numbers match when trying to find that customer across providers. This is also true when trying to tie a customer identity across traditional marketing channels, email, and affiliate marketing programs. Many companies provide anonymous identity matching to solve this problem, with LiveRamp being the largest. Often, these same companies also have access to consumer data that can be linked by their unique identifier to an individual's identity graph.

   To build this graph, companies provide their CRM data to these connectivity providers through a process known as "on-boarding." This is both a time consuming and painful process. Moreover, it potentially exposes their CRM data to others and thus creates a security risk. But customers are willing to do so because companies like Acxiom, Nielsen, Experian and others act as trusted third parties who have reputations for handling customer data with great care for privacy and security.

   Given blockchain's economics, these services are natural targets for a blockchain-based approach. In this case, companies share identities anonymously (using hashing algorithms) directly with other peers on a blockchain network on an as-needed basis. The network then uses consensus-based algorithms to create a larger and larger identity graph over time accessible through the public ledger based on these completely anonymized hashes. Any member of the network can then use the complete identity graph to personalize offers across all delivery channels connected to the network. This reduces the role of the trusted third party to one of providing intelligence (i.e. the algorithms) to the network for identity matching without the onboarding overhead, thus lowering the cost of maintaining the identity graph – or at least that is what many publishers hope blockchain will deliver. Several technologies are already being examined and/or tested. These include Enigma[14], uPort[15], Sawtooth[16], and Sovrin.[17]

[14] See https://www.enigma.co, in particular the white paper "Enigma: Decentralized Computation Platform with Guaranteed Privacy."

[15] See https://www.uport.me/, especially their white paper on self-sovereign identity at https://whitepaper.uport.me/uPort_whitepaper_DRAFT20170221.pdf.

[16] Sawtooth is being used by PokitDoc and the DokChain Alliance as the basis for their Identity by Consensus platform in the health care space. See https://dokchain.com/download/whitepaper/.

[17] See https://sovrin.org/. Hyperledger Indy is a new project on the Hyperledger platform that looks like it will leverage the Sovrin framework, as well.

3. Reducing the Power of the Large Publisher Networks. Google and Facebook now represent over 75% of all ad spend worldwide.[18] Part of this is due to their reach – Facebook has over 1.5B users worldwide, for example – which is impossible to ignore. But another is that the ability of advertisers to create similar reach at a competitive ROI through a multi-channel aggregation strategy is difficult and costly, as noted in Figure 4. In the case of Facebook and Google, their integrated exchange platforms make setting up ad campaigns or generating filled publisher units both easy and cost- effective. The overall average cost as a percentage of ad spend for using DFA is 30% for online display.[19] Aggregation of similar audiences through "open channels" costs 40% for online display, not including the cost of additional customer segment data. Extra cost and extra effort is not a good business model for success against the larger networks.

   Blockchain potentially offers an opportunity disrupt the current business dynamics of the large publisher networks in favor of an "open channel" strategy. A combination of forces related to cryptoeconomics would have to emerge to make this possible. But it is not out of the question, given the product concepts already in development.

   As an example of one possible scenario: a shared ledger would need to fulfill the promise of removing layers and costs from the existing open channel value chain. Then, on the other side of the ledger, something like the Brave browser and its Basic Attention Token would allow consumers to easily control their privacy preferences around what ads they wish to see and get paid for ads they do view. This would change the economics in favor of the open channels because Google and Facebook's entire business model is predicated on consumers providing free access to their personal data. The net would be that some of the savings from streamlining and simplifying the "open channel" value chain could be used to pay consumers, allowing a serendipitous model that would effectively fund itself. This would create the classic case for disruptive innovation as defined by Clayton Christianson in The Innovators Dilemma. In that model, a less feature-rich product with some unique properties that is brought to market at a lower cost can succeed because the incumbent players cannot reduce price enough to compete at the low end. This price umbrella would allow the new entrants to grow and succeed, in this case ultimately challenging the larger publisher networks.

4. Accounting Between Layers Is Problematic. Ledgers are designed to act as a system of record for transactions. But today, there is no good system of record for impressions served across the programmatic universe. Reconciliation of impressions served between an advertiser's measurement platform (like Omniture) and a publisher or a DSP and a publisher, is a painful, time-consuming manual exercise and often yields a "lets split the difference" compromise that makes no one happy.

[18] "AdTech Funding Drops in Face of Facebook-Google Duopoly." (Financial Times, January 3, 2017). https://www.ft.com/content/c4c358ca-c6af-11e6-8f29-9445cac8966f.

[19] All numbers in this paragraph are derived from conversations with advertisers and publishers active in the display markets in the last two years. The numbers are averages, and the percentage varies widely depending which products the advertiser uses and the size of account. For example, in the Google suite these could include Campaign Manager, Bid Manager, Search or Studio.

With blockchain's shared, immutable public ledger, the issue of reconciliation becomes a non-issue, since in an ideal situation every impression is recorded in the shared ledger as it is served. There is no need for reconciliation, since all ledgers agree from the outset.

5. Taxonomy Standardization is Difficult. If there is one operational problem that has truly vexed the advertising industry it is standardizing taxonomies between participants' data sets. The Interactive Advertising Bureau (IAB) has at least two on-going working groups that are constantly providing standards and seeking solutions for these problems because they have been so intractable and expensive for their members. There are two forms of this. First, on the transactional side of programmatic, things like names or abbreviations of advertisers and publishers in the transactional record do not match. One partner may have an advertiser listed as Pepsi (the brand), and another PepsiCo (Pepsi Corporation) because that is how they were listed in the signed insertion order and then transferred into the DSP. Second, audience taxonomies between data brokers, partners and others almost never match. What one vendor labels as an "AGE" field, another labels as "AGE_OF_HH", and another "Age Head of Household." Blockchain could offer an incredibly simple way to reconcile taxonomies automatically through a shared ledger and "taxonomy by consensus" algorithms.

6. Ad Fraud is a Huge Problem. Ad fraud cost programmatic display advertisers approximately $7.2B in 2016, which represents a substantial percentage of programmatic display spend outside Google AdWords and Facebook.[20] A goodly portion of this fraud is created by botnets that redirect traffic from valid sites to sites never seen by humans. Blockchain solutions are already being proposed for this problem. The AdChain Registry uses smart contracts on the Ethereum blockchain to store domain names accredited as non-fraudulent by holders of cryptocurrency in AdChain, known as AdChain Tokens or ADTs. AdToken holders play an incentivized voting game to determine whether an applicant to the registry is a legitimate, reputable publisher. Token holders realize no upside for the volume of impressions served to publishers in the registry. Rather, they realize upside by seeing the number of publishers applying to and renewing listings in the registry increase.

PRIVACY MEETS CRYPTOECONOMICS

The other side of the marketing/advertising supply chain faces the consumer who ultimately views ads. This is an area that offers equally interesting opportunities for disruption of the current business model. This is due to two factors. The first is the highly inconsistent nature of the relationship between the consumer and their online privacy. The second is the reduction in complexity and cost of delivery of new models offered by blockchain-based approaches.

[20] Augustin Fou in "Advertisers, Agencies and Publishers Need to Fight a Common Enemy -- Bad Guys -- Not Each Other" (Ad Age, April 18, 2017) http://adage.com/article/digitalnext/ad-fraud/308671/ suggests it could be as high as 60%, if you believe his logic. However you estimate it, it is a significant portion of open channel display ad spend.

The Consumer's Relationship to Privacy

The "average consumer" consistently tells researchers that controlling what personal data is available for use by marketers is highly important to them.[21] Forrester Research issued a study recently that suggested that 55% of the US online population desires to actively manage their data sharing or, alternately, their privacy settings.[22] Yet only a small percentage of these do so.[23] Just in terms of using the existing simple tools to manage even one feature of the privacy management challenge, today:

- Only 8-15% of users worldwide have ever set the "Do Not Track" setting in their web browser.[24]
- 60 percent were aware that they could delete cookies, cache or browsing history to help protect their privacy online; just 53 percent did.
- 43 percent were aware that they could turn off smartphone location tracking; only 29 percent did.
- 43 percent were aware they could change their social media account settings; only 24 percent did.
- 33 percent were aware they could read privacy policies; just 16 percent did.[25]

It requires almost herculean efforts to take extensive control of privacy settings. It requires knowing about multiple sites, then visiting each and deciphering the opt-out process. Some of the process is online, some by phone, and some requires physically mailing-in information.[26] This process is so time consuming that only the most dedicated privacy-conscious consumers are willing to discover and manage all these channels. And even with this much effort consumers cannot capture all the "leakage points" for their personal data. This is because some third-party collection mechanisms, such as an embedded AddThis widget, are collecting extensive data for a third-party without being obvious to the consumer.

[21] Aa an example, an IDC survey found 84% of U.S. consumers are concerned about the privacy of their personal information, with 70% saying their concern is greater today than it was a few years ago. Reported in Hamblin, Matt. "Privacy Worries Are on the Rise, New Poll of U.S. Consumers Shows." (Stratford University: Curious, February 7. 2013). http://curious.stratford.edu/2017/02/07/privacy-worries-are-on-the-rise-new-poll-of-u-s-consumers-shows/. Another example: according to the TRUSTe U.S Consumer Privacy Report, about 92% of the U.S internet users worry about their privacy online, 83% are reluctant to engage with online ads and 80% will not use an app they believe won't protect their privacy. See https://www.trustarc.com/resources/privacy-research/ncsa-consumer-privacy-index-us/.

[22] Khatibloo, Fatemeh and Fleming, Gina. "Introducing Forrester's Consumer Privacy Segmentation." (Boston: Forrester Research, December 14, 2016).

[23] Similar breakouts go all the way back to 2001. See for example, Spiekermann, Sarah, et.al. "E-privacy in 2nd Generation E-Commerce: Privacy Preferences versus actual Behavior." EC '01 Proceedings of the 3rd ACM conference on Electronic Commerce. (Tampa, FL: Association of Computer Machinery, 2001, pp. 38-47), p. 42.

[24] "How Many of Your Users Set 'Do Not Track'?" (Quantable, February 12, 2015). https://www.quantable.com/analytics/how-many-do-not-track/. Also see the Mozilla blog here: http://monica-at-mozilla.blogspot.com/2013/02/writing-for-98.html. In an interesting comment as to why Mozilla's DNT rate is only 8%, the Quantable article states "Geography aside, the answer is that IE 10 & 11 default to having DNT set to on."

[25] "2016 TRUSTe/NCSA Consumer Privacy Infographic – US Edition." https://www.trustarc.com/resources/privacy-research/ncsa-consumer-privacy-index-us/

[26] See Dixon, Pam and Gellman, Robert. "Consumer Tips: World Privacy Forum's Top Ten Opt Outs." (Washington, DC: World Privacy Forum, updated May, 2017). https://www.worldprivacyforum.org/2015/08/consumer-tips-top-ten-opt-outs/.

There is also a tendency towards privacy "habituation." When the Internet first appeared, online privacy was an intensely visible issue. Over time, concerns subsided as consumers became comfortable with the medium. In 2006, for example, Facebook launched its "News Feed" feature. By making public previously searchable (but obscure) information, News Feed generated backlash. But outrage waned, and now News Feed is a central feature of Facebook. The advent of mobile yielded another spike in concern. Writers expressed that consumers felt mobile devices were a more personal platform and thus more subject to privacy concerns.[27] And while mobile privacy is still much in the minds of consumers, this concern has also subsided over time.

The result of such factors – and these are only a few that have been identified [28] - is that less than 1% of consumers engage in a meaningful, comprehensive way with their online data privacy consistently over an extended period.[29] In other words, consumer apathy has become baked-in to the existing privacy model for online commerce and social sharing.

Numerous industry pundits have suggested that consumers would be more interested in managing their privacy exposure comprehensively if tools could reduce the complexity of privacy management to a few straightforward settings on an online portal. An associated hypothesis is that consumers could be incentivized to adopt such a service if paid for the use of their data for marketing or other purposes.

In the blockchain world, the business model around the Basic Attention Token (BAT) from Brave is based on these assumptions. BAT allows advertisers to cost effectively deliver ads and pay consumers for watching them in millicents per ad viewed.

Sadly, experience over an extended period shows that only a small cadre of consumers have shown interest in comprehensively managing their privacy preferences for online marketing data. Numerous online ventures have offered a service for just this purpose and failed.[30] Current venture-funded startups like Hitbliss, Wonder and RewardTV have yet to break through and are still unproven quantities.

Given these facts, it is hard to believe that consumers could be convinced to spend substantial time managing and monitoring a tool around a topic about which they are apathetic.

Yet academic research shows that consumers will often trade their data for very small rewards.[31] Moreover, the existing online advertising model proves consumers place an implicit value on content, because they

[27] As one example, see mtucker, "FTC: Consumer Privacy on Mobile Devices." (adMonsters, November 5, 2012). https://www.admonsters.com/ftc-consumer-privacy-mobile-devices/.

[28] Leslie, John. "We Say That We Want Privacy Online, But Our Actions Say Otherwise." (Boston: Harvard Business Review, October 16, 2015). https://hbr.org/2015/10/we-say-we-want-privacy-online-but-our-actions-say-otherwise.

[29] To be clear, consumers may opt-out or opt-in to one or more sites or programs on any given day. But consumers as a rule do not examine the privacy exposure holistically and attempt to control an overall imprint available to third-parties.

[30] These include companies like Handshake, Singly, and Personal, none of which exist today.

[31] Hann, Il-Horn, et. al. "Online Information Privacy: Measuring the Cost Benefit Tradeoff." Also see Morey, Timothy, et. al. "Customer Data: Designing for Transparency and Trust." (Boston, Harvard Business Review, May 2015) which states the results from an extensive survey of 900 people "Our surveys reveal that when data is used to improve a product or service, consumers generally feel the enhancement itself is a fair trade for their data."

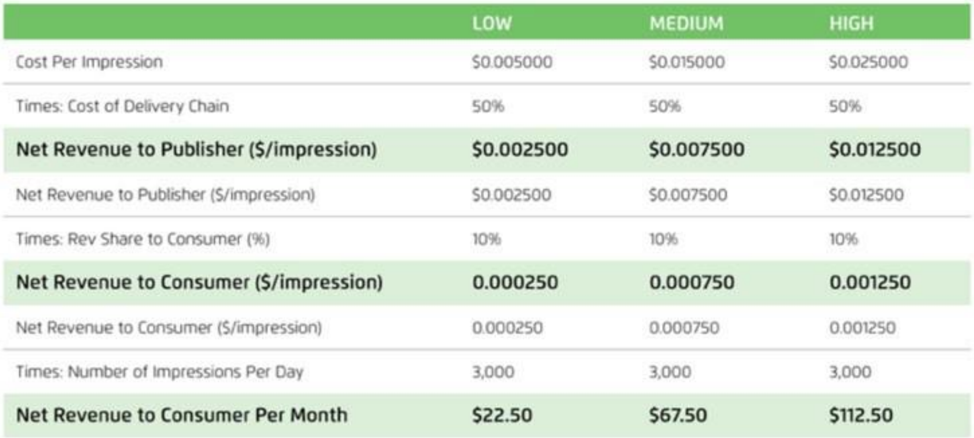
have generally been willing to trade their attention, and to a certain extent their browsing behavior, for free content. Putting a number to this implicit value is difficult, but we know it exists because when advertisers abuse the implicit agreement they have with consumers, either by serving too many ads, by creating an annoying ad experience, or by having ads “stalk” the consumer via retargeting, consumers install ad blockers to rebalance the economic exchange.[32]

We also know they value special offers, coupons, lotteries and other monetary incentives online because they sign up and trade substantial amounts of personal data (in many cases) to get a deal on products or services they value. A recent study from Nielsen Media Labs commissioned by the Jun Group found that a plurality of respondents prefer value-exchange offers - that is, rewards-based ads.[33] But, once again, the exact dollar value required to convince a consumer to trade information is not a straightforward calculation. Numerous elements enter consumers’ valuation model that determines how much they expect to receive in return for sharing. An example is brand reputation. Consumers will share data with trusted brands at a lower cost versus sites and brands that are less well known. They will also discount their data value for sites/brands that provide clear and strong privacy protections.[34]

The form of value exchanged is also a critical factor, and it goes to the heart of a pay-for-attention model. The simpler the offer is to quantify, the more likely the exchange will occur. Hitbliss users watch three video ads to get access to one movie online. The alternative is to pay $9.99/month for Netflix for unlimited content. A consumer can quickly calculate how many movies a month they may watch and determine if the inconvenience of watching ads offsets the cost associated with a Netflix subscription.

The problem with any millicents per transaction model is that consumers have almost no familiarity with it. Moreover, it is unclear how much money they can or will make for their participation, and the level of effort needed to estimate the amount is beyond most consumer’s capability because it involves understanding advertising concepts like cost per thousand.

Figure 5 - Calculation of Revenue Earned by a Consumer in a Millicent Per View Advertising Model



	LOW	MEDIUM	HIGH
Cost Per Impression	$0.005000	$0.015000	$0.025000
Times: Cost of Delivery Chain	50%	50%	50%
Net Revenue to Publisher ($/impression)	**$0.002500**	**$0.007500**	**$0.012500**
Net Revenue to Publisher ($/impression)	$0.002500	$0.007500	$0.012500
Times: Rev Share to Consumer (%)	10%	10%	10%
Net Revenue to Consumer ($/impression)	**0.000250**	**0.000750**	**0.001250**
Net Revenue to Consumer ($/impression)	0.000250	0.000750	0.001250
Times: Number of Impressions Per Day	3,000	3,000	3,000
Net Revenue to Consumer Per Month	**$22.50**	**$67.50**	**$112.50**

[32] See Coleman, Arthur. “Ad Blocking Point of View.” (Redwood City, CA: Acxiom Corporation, November 9, 2015), pp. 6-9.

[33] “Most People Want to Be Rewarded After Watching an Ad Online.” (eMarketer, January 25, 2017). https://www.emarketer.com/Article/Most-People-Want-Rewarded-After-Watching-Ad-Online/1015111.

[34] Teo, H.H. Wan, W, and Li. L. “Volunteering Personal Information on the Internet: Effects of Reputation, Privacy Initiatives, and Reward on Online Consumer Behavior.” Proceedings of the 37th Hawaii International Conference on System Sciences - 2004 (Washington, DC: IEEE, 2004)

Figure 5 shows the potential monthly revenue from viewing ads for a single consumer, based on being exposed to 3,000 ads/day [35], a 50% expense associated with the ad tech value chain, and a 10% revenue share with the consumer from the remaining value (leaving the publisher 40%, or better than what they are getting today). The result is a range of income from $22.50/month to $112.50/month depending on the CPM ranging from $5 on the low end to $25 on the high end.

These amounts would probably convince early adopters to manage more extensive privacy preferences for their personal data, as long as the amount of time needed was minimal and the result effective –meaning it delivered the promise of privacy control that the consumer requires. But any interface that required identifying specific sites for sharing (out of thousands), advertisers for data sharing (out of thousands), or third- party platforms for data access would be unlikely to succeed. That has certainly been the experience to date.

The Cost of Delivering a New Privacy Model

The second issue with this model is the cost of delivering its functionality. While it is relatively easy to track how many impressions were served to a consumer in a specific browser, it is much more difficult to track sources. Every ad may be delivered from one of a hundred ad networks or direct advertisers. Reconciliation for what is owed to a viewer from each ad network, or direct advertiser, delivered via a DSP to an SSP through an exchange and some audience connectivity layer, is a potential nightmare. The same goes for billing and collecting funds. This is extremely problematic from the consumer's perspective. My advertising "wallet" would show I have watched so many ads and earned $X at the time the ads were served. However, after reconciliation, I might have only earned $X-e or perhaps $X+e, where e is the reporting error. This would create doubt about the numbers' accuracy as well as create a poor user experience that would drive consumers away. To date, these issues have made this model impractical.

Blockchain Can Solve the Privacy Dilemma

Blockchain, with the BAT model being only one of several options, potentially offers enabling capabilities that overcome these issues. On the one hand, a distributed ledger can make it easy for a consumer's preferences to propagate across any partner on the blockchain network. Each "preference set" is set as a transaction in the blockchain associated with a given user ID. When an ad is to be served, the publisher checks their copy of the ledger for the preferences associated with a given user's ID. They then request a category of ad from the advertising exchange matching the consumer's preferences and, in an alternate implementation, rejects ads not matching those preferences.

The incentive for a publisher or partner to join the blockchain is that they can charge more for an ad served because they have 100% certainty of the audience they are delivering. This is because the preference is directly stated by the consumer, not inferred from some propensity model or device id.

[35] The 3,000 ads/day number is low relative to numbers quoted by numerous sources. An example: Story, Louise. "Anywhere the Eye Can See, It's Likely to See an Ad." New York Times, January 15, 2007. http://www.nytimes.com/2007/01/15/business/media/15everywhere.html. Or Johnson, Caitlin. "Cutting Through Advertising Clutter." CBS News, September 17, 2006. https://www.cbsnews.com/news/cutting-through-advertising-clutter/

On the other side, the blockchain ensures that all members agree on what ad was served, when, at what price, and what is due to the consumer. This reduces reconciliation and billing costs, since the price paid by the advertiser is transferred to the publisher and the fee paid to the consumer at the time the ad is served. The consumer experience is preserved because the entire process is transparent to the consumer, they receive their payments immediately, can see their exact balance in real time, and spend that income immediately as they see fit. The currency of that payment can be in loyalty points, blockchain-based tokens, cash, or other incentives that customers value.

CONCLUSION

Blockchain is in its infancy. Blockchain 1.0 is going to see a wide range of technologies and business models proposed and funded, but only very few will prove themselves economically viable long term. With over 450 companies already having raised $1.5B in funding and more coming daily thanks to the new and largely unregulated Initial Coin Offering (ICO) market, our customers would be wise to carefully evaluate companies, technologies and business models. You will be better off investing small amounts in multiple ideas at this point, rather than investing a large amount into one or two big ideas. We believe there are six areas our customers should consider for investment where blockchain's earliest impact will be felt in ad tech: anonymized self-sovereign identity, campaign reconciliation and accounting, ad blocking, taxonomy management, simplification of the ad tech value chain along with (and separately) the potential disruption of the large publisher networks, and consumer-centric privacy.

Whether you believe that blockchain will have a major impact on your business, you should still be tracking it, understanding it, and testing it. We do not doubt that blockchain will significantly impact ad tech markets, but which use cases will prove most easily and economically converted to the new platform in what time frame remains very much in question. To make a timely transition once the technology proves itself requires enough experience with the new paradigm to imagine concepts that take advantage of blockchain's game-theoretical foundations. This could be a two-step process. First, begin developing your team's understanding of blockchain's essentials by porting some existing functionality onto the new platform. This will expose you to fundamental elements of designing and deploying a blockchain-based solution. Then take that success and reengineer it to take advantage of a decentralized paradigm with no trusted third-party as a central requirement. Alternately, find a partner specializing in blockchain solutions to help accelerate your understanding and deployment of a blockchain POC. Most of these will be small companies long on good ideas but short on production-grade implementations.

It is rare when a technology comes along that has the potential to alter the entire economic landscape across multiple industries. And when they do, it is an amazing transition to participate in: fast, constantly changing, unpredictable, thoroughly enjoyable, and incredibly profitable if you are one of the lucky few who 'get the model right'. Blockchain is one of those. So enjoy the ride, but make sure to pay careful attention to the costs and the risks. This is a technology market with no guardrails, so to succeed and thrive you will have to put up your own. Keep them narrow, spend carefully, and stay focused on a few key destinations. If you follow these principles, you will be well-positioned to take advantage of the new paradigm once its true value to your business becomes clear.

RECOMMENDED READING

General Reading

Bennett, Martha. “Blockchain: Miracles Remain in Short Supply.” (Boston: Forrester Research, March 2, 2017)

Buterin, Valerik. *‘Why Cryptoeconomics and X-Risk Researchers Should Listen to Each Other More.”* Medium.com. https://medium.com/@VitalikButerin/why-cryptoeconomics-and-x-risk-researchers-should-listen-to-each-other-more-a2db72b3e86b [Accessed 27 Aug. 2017].

Howard, George. “What is Blockchain Technology? A Step-by-Step Guide for Beginners” Blockgeeks. https://blockgeeks.com/guides/what-is-blockchain-technology/.

K. “Cryptoeconomics for Dummies Part 0. Medium.com. February 22, 2017 https://medium.com/@j32804/cryptoeconomics-for-dummies-part-0-7172efa81507.

Szabo, Nick. “Formalizing and Securing Relationships on Public Networks.” First Monday, Volume 2, Number 9, September 1, 1997. http://ojphi.org/ojs/index.php/fm/article/view/548/469.

Szabo, Nick. “Money, Blockchains, and Social Scalability.” Unenumerated blog, February 9, 2017. http://unenumerated.blogspot.in/2017/02/money-blockchains-and-social-scalability.html.

Tomaino, Nick. “Cryptoeconomics 101.” Medium.com, June 4, 2017. https://thecontrol.co/cryptoeconomics-101-e5c883e9a8ff.

Wang, Kyle. “Cryptoeconomics: Paving the Future of Blockchain Technology.” Hackernoon.com, June 21, 2017. https://hackernoon.com/cryptoeconomics-paving-the-future-of-blockchain-technology-13b04dab971

Wright, Aaron and De Filippa, Primavera. “Decentralized Blockchain Technology and the Rise of *Lex Cryptographia*.” (Boston: Berkman Center for Internet and Society, Harvard Law School, 2015)

AdTech Blockchain

“Basic Attention Token: Blockchain-Based Digital Advertising.” (San Francisco: Brave Software, May 29, 2017). https://docs.google.com/viewer?url=https%3A%2F%2Fbasicattentiontoken.org%2FBasicAttentionTokenWhitePaper-4.pdf

Golden, Mike, Soleimani, Ameen, and Young, James. “The AdChain Registry.” (Santa Monica: MetaXchain, 2017). https://adtoken.com/uploads/white-paper.pdf.

Blockchain and Identity

Ellison, Carl. “Establishing Identity Without Certification Authorities.” In Proceedings of the Sixth USENIX Security Symposium. (San Jose: USENIX, July 1996). http://irl.cs.ucla.edu/~yingdi/pub/papers/Ellison-OldFriend-USENIX-Security-1996.pdf.

Tobin, Andrew and Reed, Drummond. “The Inevitable Rise of Self-Sovereign Identity.” (The Sovrin Foundation, September 29, 2016). https://sovrin.org/library/.

Zyskind, Guy, Oz, Nathan and Pentland, Alex. “Enigma: The Decentralized Computation Platform with Guaranteed Privacy.” Boston: Enigma Company, June 10, 2015). https://www.enigma.co/enigma_full.pdf

Privacy

Fairfield, Joshua. “Smart Contracts, Bitcoin Bots, and Consumer Protection.” (Lexington, VA: Washington and Lee Review Online, September 2014.) http://scholarlycommons.law.wlu.edu/cgi/viewcontent.cgi?article=1003&context=wlulr-online.

Khatibloo, Fatemeh and Fleming, Gina. “Introducing Forrester’s Consumer Privacy Segmentation.” (Boston: Forrester Research, December 14, 2016).

John, Leslie K. “We Say We Want Privacy Online, But Our Actions Say Otherwise.” (Boston: Harvard Business Review, October 16, 20150

Li, Han, Sarathy, Rathindra, and Xu, Heng. “The Role of Affect and Cognition on Online Consumers’ Decision to Disclose Personal Information to Unfamiliar Online Vendors.” (New York: Decision Support Systems, Elsevier Press, June 2011).

Spiekermann, Sarah, et. al. “E-privacy in 2nd Generation E-Commerce: Privacy Preferences versus Actual Behavior.” Proceedings of the 3rd ACM conference on Electronic Commerce, October 14-17, 2001. (Tampa, FL: Association of Computing Machinery).

Teo, Hock Hai. “Volunteering Personal Information on the Internet: Effects of Reputation, Privacy Initiatives, and Reward on Online Consumer Behavior.” Proceedings of the 37th Hawaii International Conference on System Sciences, 2004. (Washington DC: IEEE).

Zyskind, Guy, Oz, Nathan and Pentland, Alex. “Decentralizing Privacy: using Blockchain to Protect Personal Data.” (Boston: MIT Media Lab, 2014)

Technical Underpinnings

Buterin, Vitalik, and Poon, Joseph. “Plasma: Scalable Autonomous Smart Contracts (Working Draft).” (Ethereum Foundation, August 11, 2007). https://docs.google.com/viewer?url=http%3A%2F%2Fplasma.io%2Fplasma.pdf.

Buterin, Vitalik. “A Next Generation Smart Contract and Decentralized Application Platform.” (Ethereum Foundation, January 23, 2014). https://bitcoinmagazine.com/articles/ethereum-next-generation-cryptocurrency-decentralized-application-platform-1390528211/

Cachin, Christian. “Architecture of the Hyperledger Blockchain Fabric.” (Zurich: IBM, July 2016). https://pdfs.semanticscholar.org/f852/c5f3fe649f8a17ded391df0796677a59927f.pdf.

Fedotova, Natalya and Veltri, Luca. “Byzantine Generals Problem in the Light of P2P Computing.” Presented at IEEE Conference on Mobile and Ubiquitous Systems, July 17-21, 2006.

Lamport, Leslie, Shostak, Robert and Pease, Marshall. “The Byzantine Generals Problem.” ACM Transactions on Programming Languages and Systems, Vol. 4, No. 3, pp382-401. (Washington, DC: Association for Computing Machinery, July 1982).

Nakamota, Satoshi. “Bitcoin: A Peer-to-Peer Electronic Cash System.” (London: www.cryptovest.co.uk October 31, 2008)

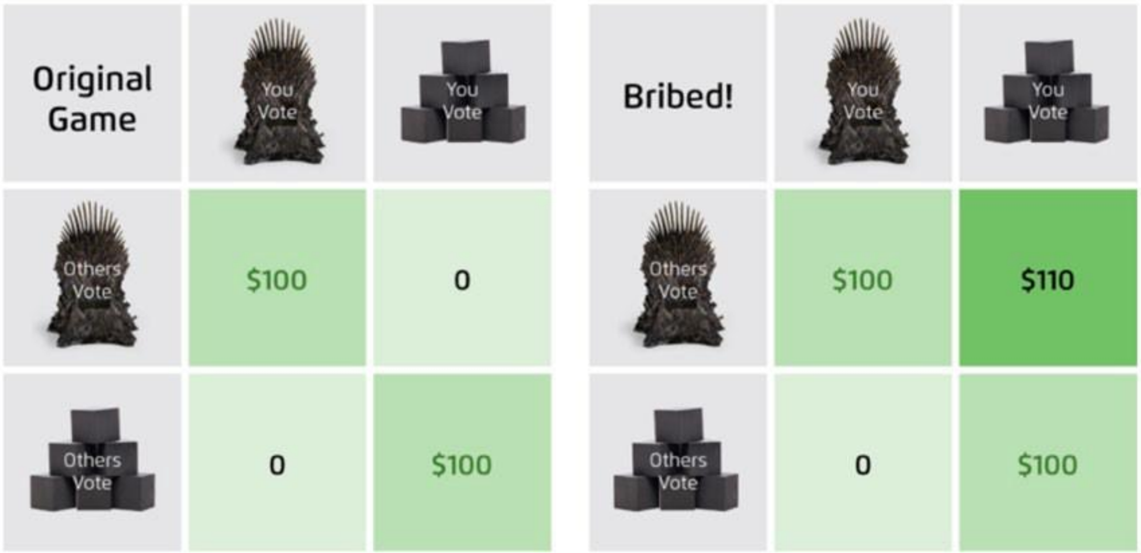
APPENDIX A – A GAME THEORY EXAMPLE [36]

Ethereum has four different models for human behavior that provide fundamental assumptions about how the Ethereum system should be designed to prevent cheating. One of these is known as the Bribing Attacker Model. It describes a game where participants in the game do not coordinate with each other and have their own goals. The model also assumes that an attacker exists with enough resources to incentivize other participants to take certain actions through conditional bribes.

Imagine there exists a game of thrones. Participants in the game will vote on whether they want to sit on an iron throne or a Styrofoam throne. Everyone who voted in the majority will win $100, while everyone in the minority will get nothing. In this game, the assumption is you would vote to sit on the Iron Throne because you want to rule the Seven Kingdoms and because sitting on a Styrofoam block sucks. You also believe the majority will do this for the same reasons. Since everyone else arrives at the same conclusion you do, the majority vote will go toward sitting on the Iron Throne and everyone will collect $100.

However, let's say a malicious Styrofoam executive is out to promote his non-biodegradable wares. In a fit of cunning, he sends everyone a conditional offer: "Vote for the Styrofoam block, and if you're in the minority I will personally give you $110!" Because he has a long history of always paying his debts, everyone knows that he is good for this commitment and has the budget to pay it.

Figure 6 - Diagrams Showing a Player's Payout Depending on the Actions Taken in the Game of Thrones



Original Game	You Vote (iron throne)	You Vote (Styrofoam)
Others Vote (iron throne)	$100	0
Others Vote (Styrofoam)	0	$100

Bribed!	You Vote (iron throne)	You Vote (Styrofoam)
Others Vote (iron throne)	$100	$110
Others Vote (Styrofoam)	0	$100

[36] Taken from Wang, Kyle, "Cryptoeconomics: Paving the Future of Blockchain Technology", July 21, 2017. https://hackernoon.com/cryptoeconomics-paving-the-future-of-blockchain-technology-13b04dab971.

Suddenly, the equilibrium shifts. Now it makes sense for you to vote for the Styrofoam throne — if you're in the majority, you collect $100, but if you're in the minority, even better, you'll walk home with $110. Since everyone else again arrived at the same conclusion you did, the majority will vote for the Styrofoam and the executive will allow himself a hearty chuckle, not having to pay out at all and achieving his goal at zero cost. Truly, his threat of benevolence was his masterstroke.

This is formally known as the P + epsilon Attack, and it turns out the Bitcoin protocol is susceptible to this strategy. However, it has not been exploited in practice because of Bitcoin's Proof-of-Work algorithm, which makes the cost of exploiting this hole so large as to make it unlikely that a bad actor will pursue such an attack.

About the Author

Arthur Coleman is General Manager of Acxiom Research, where he leads a team of engineers and data scientists. These teams conceive and develop intelligent products that can generate new revenue sources for Acxiom by creating discontinuous change in our industry.