



# The AdChain Registry

May 31<sup>st</sup>, 2017

Mike Goldin  
ConsenSys

Ameen Soleimani  
ConsenSys

James Young  
MetaX

# Introduction

The unwitting purchase of bot traffic in digital advertising markets defrauds advertisers of over \$16+ billion annually.<sup>1</sup> Opaque supply chains provide cover for botnet operators who hide behind the black boxes of exchanges and deep within un-auditable ad networks.<sup>2</sup> Because supply chain entities downstream from the advertiser are generally paid on a cost per mille (“CPM”) basis, their incentive alignment is towards maximizing impressions irrespective of whether those impressions are from human eyeballs or bots. Because botting is cheap and hard to detect, it may even be economically rational for downstream entities to knowingly serve ads to bots.

Ad buyers are increasingly frustrated by having their money stolen.<sup>3</sup> While programmatic ad buying is undoubtedly the path forward for quantifying the value of ad buys relative to direct dealing and is the highest growth area of digital advertising, programmatic is, at present, a morass for quantifying efficacy in advertising non-installable goods.<sup>4</sup> The behaviors of humans on web pages are easily mimicked by bots and the flagging of bot network signatures is essentially a cat and mouse game.<sup>5</sup> This leaves advertisers mostly powerless against the incentive structure of the downstream supply chain.

The adChain Registry is a decentrally-owned domain whitelist being launched as a collaboration of ConsenSys, MetaX, and Data & Marketing Association (DMA), an industry group with 1,400 active members and over 100,000 participants. adToken holders play an incentivized voting game to determine whether an applicant to the registry is a legitimate and reputable publisher or not. 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. So long as the registry is kept clean of bot traffic, advertisers will want to service bid requests from its registrants. So long as advertisers desire to service bid requests from registrants, registrants will desire to renew their listings and unlisted publishers will desire to apply for listings. Token holders are incentivized to keep fraudulent applicants out of the registry by voting judiciously to maintain this virtuous cycle.

## The adChain Registry

The adChain Registry is a smart contract on the Ethereum blockchain which stores domain names accredited as non-fraudulent by adToken holders. The presence of the domain foo.net in the registry means that adToken holders have recently assessed that domain belongs to a legitimate publisher with a real human audience.

The Registry also exposes both an interface with which token holders propose new domains to be listed, and one to challenge such proposals. An interface for token holders to vote on outcomes when challenges are raised is also exposed.

---

<sup>1</sup> [“Ad Fraud Estimates Double”](#). WPP. Business Insider. March 16, 2017.

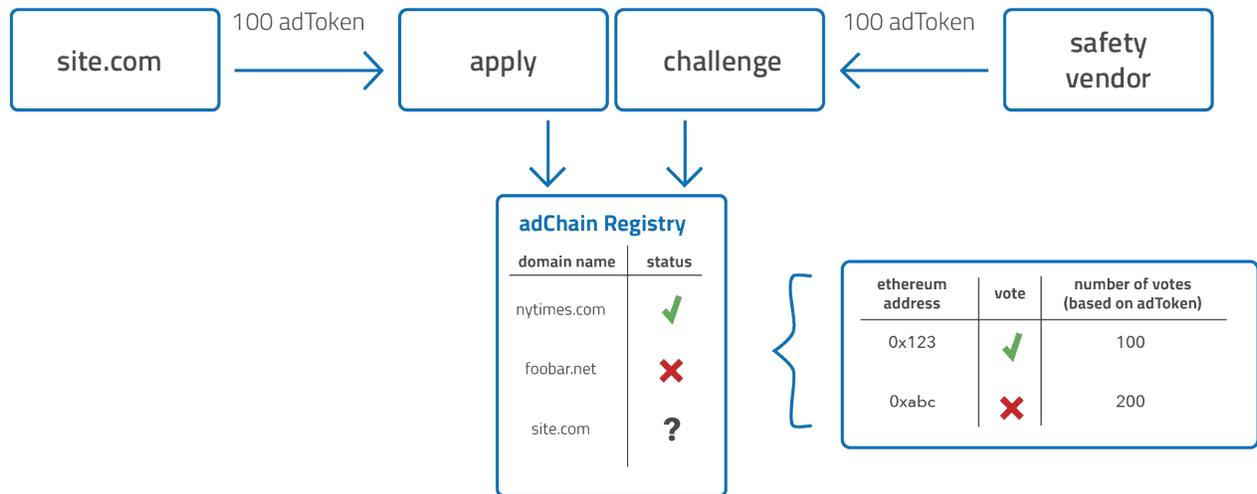
<sup>2</sup> [“The Methbot Operation”](#). WhiteOps. Page 10. December 20, 2016.

<sup>3</sup> [“Chase Had Ads on 400,000 Sites. Then on Just 5,000. Same Results.”](#). Sapna Maheshwari. The New York Times. March 29, 2017.

<sup>4</sup> [“Interview with MachineZone CEO Gabe Leydon”](#). Recode. February 24, 2016.

<sup>5</sup> [“Mystery Shopping Inside the Ad Fraud Verification Bubble”](#). Shailin Dhar. June 8, 2016.

Finally, an interface is exposed with which adToken holders can vote to reparameterize constant factors in the Registry, such as the period over which listing applications are challengeable.



### Listing Applications and Data

To apply for listing in the adChain Registry, the applicant supplies a domain name such as foo.net and an adToken deposit. The application sits in an application pool for the duration of a challenge period. If no challenges are raised against the application over the course of the challenge period, the domain is added to the Registry.

Listings in the adChain Registry are only valid for a finite period of time. Because domain names can be sold or degrade in quality over time, a high quality domain today may be low quality tomorrow. Registrants can apply to renew a listing prior to the lapse of its accreditation, and a successful renewal will cause no interruption to the domain's accreditation status. When a listing's accreditation lapses, the adToken deposit made with the original listing application can be withdrawn by the applicant.

Listings may include additional, optional metadata such as whether the registrant accepts BAT<sup>6</sup> payments or an attestation of compliance with existing industry standards.

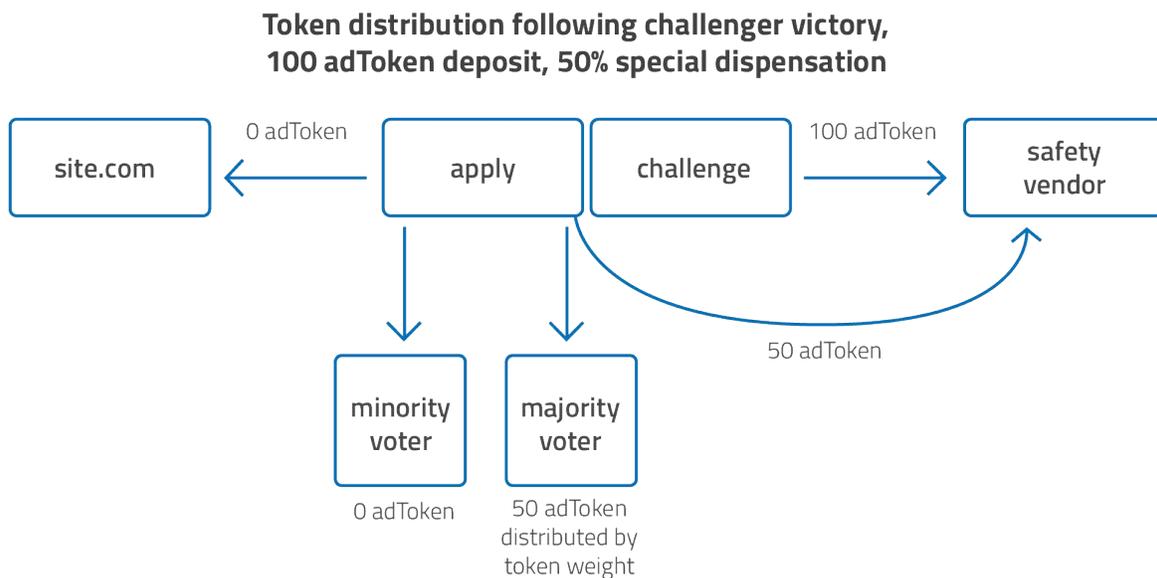
### Challenging Applications For Listing

Applications for apparently fraudulent or low quality domains will be challenged by rational adToken holders. To initiate a challenge against a listing application during its challenge period, a token holder must deposit a sum of adToken equal to the deposit made by the applicant. Doing so initiates a voting period during which token holders engage in a token-weighted vote which determines whether an applicant is to be admitted. The voting scheme is commit-reveal and derives from [Colony's partial-lock token weighted voting system](#).

<sup>6</sup> ["Basic Attention Token \(BAT\)". Brave Software. May 23, 2017.](#)

If the challenge is settled in favor of the applicant, the challenger’s deposit is forfeited and the applicant’s domain is listed in the adChain Registry. If the challenge is settled in favor of the challenger, the applicant’s deposit is forfeited and the applicant’s domain is not listed in the adChain Registry. Applicants can reapply for listing as often as they like if their application fails.

When the vote concludes a percentage of the forfeited deposit is awarded directly to the winning party in the challenge (either the applicant or the challenger) as a special dispensation. The remainder of the deposit is divided proportionally among token voters in the winning bloc by token weight. Voters in the losing bloc receive nothing.



The deposit of the winning party in the challenge is always returned to them. Tokens locked for voting are always returned to their owners regardless of whether they were cast with the majority or the minority. Only the deposit of the losing party in the challenge is redistributed and not recoverable by its original owner.

### Parameterization of the Registry

There are no constant (“magic number”) values in the adChain Registry. The Registry will be instantiated with reasonable values based on the best estimations of the creators, but all of these will be changeable by adToken holders who may vote to reparameterize the Registry. Parameterized values mentioned so far include: application deposit amounts, the duration of the challenge period, the duration of a registration’s validity, the duration of the commit and reveal periods in token votes and the size of the special dispensation made to the winning party in token votes. Parameters of the governance system itself may be votable as well, such as the share of tokens required to initiate a reparameterization.

As an example of how the parameterization of constant values in the registry affects the mechanics of the game, consider the special dispensation awarded to challenge winners. Rational actors should only

challenge listing applications based on a calculation of potential earnings, which is a function of the challenger's expected payout and confidence in winning the token vote. The challenger stands to lose 100% of their deposit if they lose the token vote, or win some amount over their original deposit if they win the token vote. If the special dispensation is set at 50%, a rational challenger must be above 66% confident in their ability to win a token vote to raise a challenge.<sup>7</sup> Thus the percentage of the applicant's deposit allocated as a special dispensation for the challenger determines the confidence level above which a rational challenger will submit challenges.

The adToken supply is non-votable, and adToken can be neither minted nor destroyed. The 1,000,000,000 adToken deployed upon instantiation will be the set number of adToken in perpetuity.

### **The Virtuous Incentive Structure Between Advertisers, Publishers and adToken Holders**

Most payments in digital advertising occur on a CPM basis. The CPM model creates misaligned incentives and is the source of many issues in the digital advertising supply chain. An advertiser pays a publisher some fixed amount per thousand impressions and this constitutes a CPM. The problem with the CPM model is that impressions are an exceptionally weak indicator of actual attention spending by viewers. This is in part due to the fact that impressions are highly abstract notions which different vendors assess in different ways. Vendors downstream from the advertiser are incentivized to assess what constitutes an impression as loosely as possible.

A malicious publisher in the advertiser to publisher example has no real incentive to report any page view as less than a full impression. Indeed, because it is so easy for bots to impersonate human behavior on web pages, it is often economically rational for a publisher to buy bot impressions and report them to the advertiser as legitimate. The advertiser is incentivized to scrutinize the impression data they receive carefully, but the task is essentially non-computable and devolves to statistical guessing. This problem is exacerbated by the large number of intermediaries in a typical programmatic supply chain. A single ad impression can transact between dozens of parties that sit between the advertiser and the publisher. The incentive structure of the publisher is identical to all those parties downstream of the advertiser, since anybody who reports fraud down the line forfeits revenue for themselves by doing so.

The key innovation of the adChain Registry is that it incentivizes the curation of a reputable supply pool by decoupling the incentives of the registry owners (adToken holders) from CPMs. Token holders have one concern, which is to flag fraudulent and low quality applicants to the pool and win votes to reject those applications. The simple schelling point for these votes is around whether the applicant is fraudulent or low-quality; voters acting rationally should settle in blocs for or against acceptance on the basis of their assessment of those qualities. Voters who act rationally and perform good diligence will be rewarded. Less diligent voters on the losing side incur opportunity cost without upside for having locked their adToken uselessly over the duration of the voting period.

A final point must be understood to close the loop on the virtuous incentive cycle between advertisers, publishers and token holders. A "meta" schelling point for voting behavior in challenges is not explicitly whether the applicant is fraudulent or not, but what outcome in the vote will increase the value of

---

<sup>7</sup> There is a 33% chance of -100% deposit and a 66% chance of +50% deposit.  $(0.33)(-1) + (0.66)(.5) = 0$ .

adToken. While this notion should be very tightly coupled to the notion of fraudulence, it is useful to consider it in its own right.

Consider that the challenge game is only available to play when there are applicants in the applicant pool. The applicant pool will only have applicants in it while publishers desire to make or renew listings in the adChain Registry. Publishers will only desire to make or renew listings in the adChain Registry while advertisers desire to service bid requests for ad space from publishers in that registry. Advertisers, in turn, will only desire to service bid requests for ad space from publishers in the adChain Registry while the Registry is considered clean relative to other ad networks and whitelists. This being the case, token holders are incentivized to keep the registry clean by initiating challenges against suspect applicants and voting to remove apparently fraudulent listings.

The game design of the adChain Registry, with its deposits and voting, has a lot in common with proof-of-stake consensus in blockchains. The key difference is that blockchains verify blocks, which is computable, while adChain verifies domains as non-fraudulent, which is not. adChain thus explores the general pattern of using collateralized consensus mechanisms to establish single sources of truth in non-computable domains. adChain does not aim to solve advertising fraud directly, it simply allows the advertising industry to agree on what fraud is, and where to draw the line.

## Practical Utilization of the Registry

The adChain Registry provides a high-quality, zero-cost whitelist from which advertisers can read to assess whether or not to service inbound bid requests on ad opportunities. The minimal contents of a listing in the adChain Registry, however, are nothing more than a domain name and an indicator of the listing's accreditation status. Assuming the absence of any authentication scheme, if foo.net is an accredited registrant in the adChain Registry a bot farm could trivially impersonate foo.net by simply changing the origin headers of their bid request messages.

Advertisers need to protect themselves from the trivial attack in which bot farms impersonate adChain registrants by spoofing origin headers. While the Registry itself is unopinionated on this matter, it will be useful for the industry to settle on a uniform way of authenticating themselves to one another. The use of bidirectional authentication using Transport Layer Security (TLS), a widely deployed and battle-tested suite of technologies, can address this. The unidirectional handshake protocols of TLS underpin authentication for HTTPS connections on the Web. Bidirectional TLS handshakes underpin authentication in the widely used SSH (Secure Shell) protocol.

This section also discusses tools which will be provided by MetaX to enable token holders to easily interact with the adChain Registry, and a partnership with Data & Marketing Association, an industry group with 1,400 active members and over 100,000 participants which has agreed to help move the project forward with the existing industry.

## Mutual Authentication Using TLS

By pushing authentication out of the application layer and into a widely used transport layer technology like TLS, adChain registrants can conduct ad commerce in RTB, VAST, VPAID or any other markup format including ones which do not exist yet. It also means existing production-ready software can be leveraged to perform the authentication, and onboarding costs for new users become as low as a few lines in a webserver config file.

Bidirectional TLS authentication using certificate signing keys in the Web HTTPS regime will suffice to authenticate users in adChain. An advertiser servicing a bid request with headers indicating an origin at `foo.net` will ask the sender to mutually authenticate in the TLS handshake. The recipient will expect authentication to be performed with a key authenticable using an SSL certificate for `foo.net` issued by a trusted Certificate Authority.

The advertiser's server implements the following branching logic:

1. Can this client perform mutual authentication over TLS?
2. If yes, did the client authenticate properly in the TLS handshake?
3. If yes, does this domain have a listing in the adChain Registry?

If the answer to any of those questions is “no”, the server branches off to execute arbitrary logic to handle that case. Supporting the authentication of adChain members does not mean advertisers must forgo business with non-adChain members.

On the supply side, entities serving bid requests must be able to authenticate in TLS sessions using the certificate signing key of the registrant whose domain listing they solicit bids for. Technically savvy publishers may choose to simply run their own ad servers to retain control of their certificate signing keys. Most publishers, however, are used to working with vendors who solicit bids and return ad markup without requiring they do anything more than embed Javascript on their webpage. Adopting mutual authentication means vendors must either apply for a listing in the adChain Registry or interface with publisher-controlled signing servers.

Rational token voters should be biased towards rejecting vendor applications because vendors aggregating supply from multiple publishers are difficult to audit and can easily hide bot traffic amongst their legitimate traffic. The signing server approach is likely a happy middle-ground: deploying a signing server should not be difficult even for relatively unsophisticated publishers who desire to retain control of their certificate signing keys, and the task can be entrusted to specialized service providers as well.

Another possibility is for publishers to simply entrust their certificate signing keys to proxies who work on their behalf. Sharing a certificate signing key requires high trust in the proxy, but sophisticated vendors may be able to build businesses using this model.

## Interfaces for Voting

While the adChain Registry will be a smart contract on the public Ethereum blockchain available for anybody's equal use, MetaX intends to provide a user interface wrapping the Registry such that token holders can participate in the voting process through a web browser. This interface will enable token holders to apply for listings, open challenges, vote in challenges and vote on the parameterization of the Registry itself. While this interface will be optional, it should make participation accessible to a much larger audience.

Because of the nature of smart contracts on public blockchains, anybody will be able to write their own GUI wrappers should they so choose. Interaction with the Registry through tools like MetaMask, MyEtherWallet, Mist or a command line will obviously work as well.

## Partnership with Data & Marketing Association

“It’s inspiring to see smart start-ups take on providing innovative solutions to challenges in our industry that are resulting in fraud and injuring marketers’ relationships with their customers. As the only trade association in marketing and advertising that represents all parts of the ecosystem equally, DMA is eager to see its members, like MetaX, provide innovative and trust-based solutions that support the client and supply sides of our industry around ad-fraud and other system-wide pain points.”

- Thomas Benton, CEO of Data & Marketing Association (DMA)

Data & Marketing Association (“DMA”) is an industry group representing over 1,400 organizations on both the demand and supply sides of the digital advertising ecosystem. DMA has agreed to advocate on behalf of adChain as well as evangelize the technology through education and training. DMA has a vested interest in making the adChain Registry a success and to stop fraud from continuing to harm its members. MetaX will be providing DMA with technical training about blockchain technology as well as marketing materials, demos and actionable metrics that prove the adChain value proposition. DMA will also serve as a proud member of the adChain Association (ACA), a nonprofit governing body formulated to oversee best practices regarding the adChain protocol.

## Project Governance

A unique feature of adChain relative to other tokenized protocols is its ambition to tackle a massive problem facing an existing industry by providing governance tools to members of that industry, and onboarding the industry starting top-down. Brave, Gnosis, Golem, Melonport, SingularDTV and the like are creating blockchain platforms to rival existing platforms but are designed to grow from the bottom-up, which certainly is a valid approach. The design of adChain was motivated from the outset by the challenge of onboarding the existing advertising technology industry. The complexity of this platform is not entirely captured in the protocol itself, but in the interaction between the protocol and existing industry players. The protocol is intentionally simple for this reason; if the system were too complex it would be too difficult for industry players to determine their place within it and optimal strategies, which would slow adoption.

This project’s governance will likely be a pivotal factor in its long-term success. ConsenSys, MetaX and DMA collectively bring to bear expertise in blockchains, digital advertising, and influence in the advertising industry itself to a project whose success will require all three.

## **Organizations Involved**

**ConsenSys** is a venture production studio building decentralized applications, systems, developer and end-user tools for the Ethereum blockchain. Founded in Brooklyn in 2014, ConsenSys is a global organization with 200 employees on six continents. ConsenSys’ enterprise consulting organization designs and builds Ethereum-based blockchain infrastructure for Fortune 10 companies. ConsenSys was the incubator for both the BlockApps and Gnosis companies. ConsenSys’ advertising technology practice which will be building applications and services around adChain is called CAT.

**MetaX** is a blockchain technology company committed to the development and adoption of open platforms for the digital advertising industry. The company is based in Los Angeles and allows the digital advertising supply chain to coordinate in a scalable, trustworthy and secure way. To sign up for company updates, please visit: <http://metax.io>

**Data & Marketing Association, About DMA** ([www.thedma.org](http://www.thedma.org)): Founded in 1917 and driving the data and marketing agenda for a full century, Data & Marketing Association (“DMA”) champions deeper consumer engagement and business value through the innovative and responsible use of data-driven marketing. The DMA’s brand-leading membership is made up of over 1,400 organizations who are today’s innovative tech and data firms, marketers, agencies, service providers and media companies. By representing the entire marketing ecosystem—demand side and supply side—and engaging more than 100,000 industry professionals annually, DMA is uniquely positioned to convene and guide the industry to bring win/win solutions to the market, and ensure that innovative and disruptive marketing technology and techniques can be quickly applied for ROI.

DMA advances the data-driven marketing industry and serves its members through four principal pillars of leadership: advocating for marketers’ ability to responsibly gather and refine detailed data to identify and fulfill customer needs and interests; innovating to bring solutions forward to the data & marketing ecosystem’s most vexing challenges; educating today’s members of the data & marketing ecosystem to grow and lead marketing organizations in the ever-increasing omnichannel world; and connecting industry participants to stay current, learn best practices and gain access to emerging solutions through &THEN – the largest global event for data-driven marketing – and DMA’s portfolio of other live events.

## **The adChain Association (ACA)**

In tandem with the launch of the adChain Registry, an independent, nonprofit, and democratic governance body for the members of the ecosystem and adToken holders will be established (ACA). The details of this non-profit entity are still being finalized and will be shared publicly once confirmed.

It’s mandate will be to give developers an open platform to develop, deliver, and enhance secondary services that will attract more and more publishers to the Registry. As time goes by it is likely that the Association will be replaced by other, more innovative governance methods such as a

decentralized autonomous organization (DAO).<sup>8</sup> Creating a formal legal body at the onset, however, is an important first step in this process.

## **Team**

### ***Mike Goldin***

Mike began working on applications for the Ethereum blockchain during the summer of 2015 as an intern at ConsenSys, where he worked on the smart contract backend for Ujo Music. He joined ConsenSys full-time after graduating from Columbia University with a degree in computer science. He worked as a software developer and architect in the ConsenSys Enterprise group and is now the technical lead for ConsenSys AdTech.

### ***Ameen Soleimani***

Ameen has been a software developer at ConsenSys since the summer of 2016. Outside of adChain, his projects include peer-to-peer energy markets, decentralized hedge funds, and state channels research. Prior to joining ConsenSys, Ameen studied chemical engineering at Rensselaer Polytechnic Institute, founded Potomoc Code Camp to teach middle schoolers programming fundamentals, and founded Filter, a personalized news reader. He is now the founder of Moloch Ventures, a blockchain venture production studio with a focus on state channels and tokenized smart contract platforms.

### ***Mark D'Agostino***

Mark has spent the past decade in management consulting, specifically focused on the financial services industry. Prior to joining ConsenSys as a managing partner in the Enterprise group, Mark built out Deloitte's blockchain market offering. He has successfully delivered Ethereum based applications to Fortune 500 banks, global energy companies and governments. Over his career, he has served clients such as AIG, BlackRock, Citi, GE, JPM, Lehman Brothers, MasterCard, and Pfizer. On the adChain collaboration, Mark drives strategy and business development.

### ***Miguel Morales***

Miguel Morales is an experienced full stack engineer focusing on product development, architecture, and agile processes. He specializes in building for large-scale systems and data management platforms. Morales has deep vertical expertise in building for the adtech ecosystem, especially mobile and programmatic-driven initiatives. He is currently a product engineer at MetaX, leading efforts on adChain initiatives and related MetaX-developed dApps. He recently worked at ZeroX and The Mobile Majority.

### ***James Young***

James has 20+ years of software development experience specializing in streaming video network design and social/mobile game development. His first startup acquisition happened when working at InterVU (the first video CDN), which was later acquired by Akamai). He has also worked at large enterprise companies like, Cisco and notable startups like Zynga. He tried to get a job at HotWired during the pre-hipster era of the internet and has been interested in the open web ever since.

---

<sup>8</sup> For instance, the Aragon project (<http://aragon.one>) presents a smart contract framework for constructing and upgrading decentralized autonomous organizations (DAOs).

***Ken G. Brook III***

A serial entrepreneur, Ken has built technology companies from the ground up since 2010. His most recent accomplishment is co-founding and serving as CEO of MetaX, the first platform to unlock the blockchain for digital advertising. Most recently, Ken founded and currently still serves as CEO of VidRoll, a video technology and monetization partner for premium content publishers. Previously, Ken started StreamRoll Media, a cross-screen adtech company, in 2013, and earlier in his career held positions in both traditional and digital media.

**Advisors**

***Raleigh Harbour***

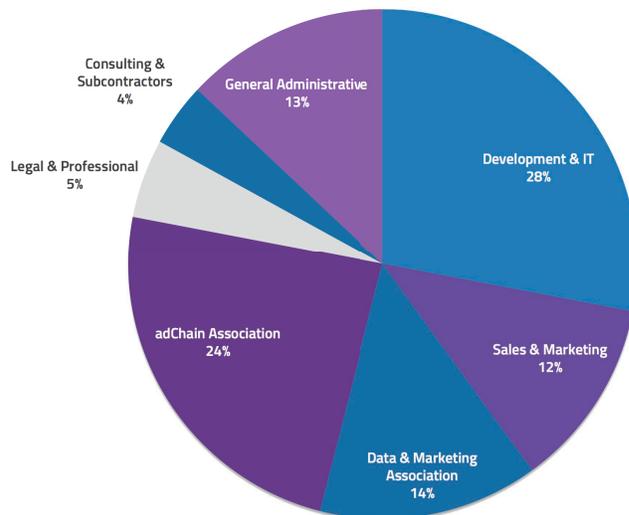
Raleigh is a seasoned executive with nearly 20 years of experience in SaaS software, online media, digital advertising, and business services. Raleigh currently serves as Managing Partner of ATON Fortis, a strategic advisory firm working with technology start-ups in the LA area. Previously, Raleigh was SVP of Client Services & Operations for AOL, leading a team responsible for transforming AOL into a scalable platform company. Raleigh joined AOL via its acquisition of Adap.tv, where he was COO, responsible for the company’s global operations. Prior to Adap.tv, Raleigh was SVP of Business & Corporate Development for the Rubicon Project. Raleigh holds a BA from the University of Virginia and an MBA from the University of Chicago.

***Shailin Dhar***

One of the few genuinely independent ad fraud consultants, Shailin is the author of Uncommon Sense for Ad Tech, an authoritative text on adtech, providing an unparalleled level of detail on the topic. Having worked years as a programmatic trader, and having gained first-hand experience in poorly understood, yet widely used practices of arbitrage and traffic sourcing, Shailin brings to the adtech industry a breadth of knowledge only few can claim. Ranging from meticulously thought out play-books for highly competitive media investment, to the dark arts of the adtech underbelly.

**Use of Proceeds**

adChain Use of Proceeds



## Roadmap

June 2017 - adToken Launch

August 2017 - Experimental Registry Deployed

September 2017 - Header bidding peer to peer exchange

October 2017 - Launch Dapp bounty program

January 2018 - Data markets

August 2018 - Challenges to registry applications are opened to all token holders

February 2019 - Full decentralization, registry applications are opened to all token holders

## Token Launch Details

The collaboration between ConsenSys and MetaX began after an introduction from a mutual friend, Yorke Rhodes, a blockchain leader within Microsoft, and has been ongoing for over a year. The platform itself has been through multiple iterations and redesigns over the past six months after receiving feedback from community members, industry participants and legal advisors. Over the past year, ConsenSys and MetaX decided to pre-sell 10% of the future tokens in order to fund development, onboard industry participants such as the DMA and their members orgs, and pay for legal analyses. The pre-sale of tokens were to specifically identified participants who have an interest in seeing the adChain platform become a transformative protocol within the advertising technology industry. The 10% of pre-sale tokens represent 100 million of the 1 billion tokens to be distributed at the public launch, contemplated to take place in late June, 2017.

The token breakdown is as follows:

- 500 million to be distributed in a public token sale with a cap of \$10 million sold
- 200 million reserved for MetaX, per the time lock schedule detailed below
- 200 million reserved for ConsenSys, per the time lock schedule detailed below
- 100 million sold to fund development via multiple pre-sale agreements (as described above)

ConsenSys and MetaX will jointly deliver on the roadmap outlined in this white paper. It is the belief of ConsenSys and MetaX that token launches in this ecosystem may be naive in selling upwards of 75% during their first “token round.” Typical startups would exhibit an even greater failure rate if they limited their startup capital to only one funding round. ConsenSys and MetaX believe it is better to sell tokens over time as i) adChain achieves its targeted adoption milestones across the digital advertising industry and ii) ConsenSys and MetaX continue to develop and release new advancements of the adChain protocol. As such, ConsenSys and MetaX believe it is in the best interest of the platform to retain 40% of the tokens after the first public sale. This gives the adChain team flexibility to initiate future token sales if warranted.

ConsenSys and MetaX plan to use part of the 40% retained tokens held in escrow as bounties for the community to build specifically desired functionality. After year one when governance is more fully fleshed out in the adChain protocol, ConsenSys and MetaX plan to post tokens in escrow and have token

holders vote on whether or not submissions satisfy requirements of our bounties - this ensures that ConsenSys and MetaX push further into decentralized control over the adChain system.

To signal the level of commitment both ConsenSys and MetaX have for this system, each entity has agreed to lock up all of their tokens with the following unlocking schedule:

- 50% unlocked 1 year after public sale
- Remaining tokens unlocked 18 months after public sale

## Future Work In adChain

The adChain Registry and TLS authentication scheme proposed is production-ready to support *server-side header bidding*. To conduct server-side header bidding means a publisher or its proxy solicits bid requests from the demand side directly, without an exchange acting as an intermediary. Server-side header bidding has been gaining traction in advertising technology independently of the rise of blockchains because it provides bid transparency to publishers and removes a middleman from the demand-supply relationship.<sup>9</sup> It works well with adChain because it is a peer-to-peer technology which maps onto many of the design patterns becoming prevalent in the emerging field of cryptosystems. One factor which has impeded the adoption of header bidding throughout the industry is the problem of “discovery”, or identifying the entity on the other side of an inbound bid request. The adChain Registry is a breakthrough for discovery in header bidding, as the bid request recipient can determine whether an otherwise unknown entity is reputable simply by authenticating it over TLS and checking whether it has an adChain listing.

A long-term objective is to bring the benefits of blockchains and the adChain Registry to users whose needs cannot be fully satisfied by server-side header bidding. Enabling discovery for client-side header bidding will be highly desirable as the web decentralizes, and supporting authentication over multi-hop supply chains will be a breakthrough necessary for the construction of fully programmatic ad-hoc supply chains. Using blockchains and content-addressed file systems to verify the delivery and display of ad markup could eliminate an entire category of ad fraud. Strong attribution of identity-linked actions is a holy grail for programmatic web advertising potentially made possible by open identity systems such as uPort.

### Discovery For Client-Side Header Bidding

Like server-side header bidding, client-side header bidding disintermediates exchanges and enables supply to engage in ad commerce with demand directly and peer-to-peer. As the name implies, client-side header bidding requests originate in the browser rather than on a publisher-controlled server. Because secrets cannot be safely stored in browsers, authenticating supply when requests originate in the browser cannot be done using bidirectional TLS. It may become feasible to utilize emerging client-side signing standards to construct something like an adChain user registry, or even do so as a function of open attestation

---

<sup>9</sup> [“Envisioning The Future In A Server-Side Header Bidding World”](#). Rachel Parkin. AdExchanger. February 1, 2017.

mappings on an existing identity system. Rather than authenticate the publisher, it should be possible to authenticate the user.

### **Deep Supply Chain Auditing**

The adChain Registry allows for advertisers to authenticate bid requesters as registrants in a clean pool of supply in a direct, peer-to-peer manner. In practice, most ad exchange today is conducted over multi-hop supply chains. Our approach for authentication using mutual TLS is not useful for authentication between entities in a supply chain which are not directly connected with one another. This is to say, one can authenticate the individual they are speaking with, but not who that individual is speaking for in-band to bidirectional TLS itself (“I am bar.net. I am working for baz.net who is working for foo.net”). To do so will require novel application-layer authentication logic involving diffs on ad markup and signature bundling.

### **Creative Verification**

A registry could be used to allow adChain members to register hashes of individual creative assets and metadata. The metadata could include the creative media type, its IAB Content Taxonomy categorization and its dimensions, for example. This registry could be used to do proactive verification of creative throughout the supply chain, or allow publishers to blacklist classes of ads by metadata.

### **Tracker Tag Registry**

A registry that allows analytics providers to register a hash of their javascript tracking tags. These tags are used to track user engagement with advertisements on web pages, but are sometimes corrupted by hackers and used as malware vectors to install ransomware on the computers of unsuspecting people surfing the web. If the adChain community could enforce a vetting process for new tracker tags, and publishers could verify tracking tags before running them, it would be harder to spread malware through advertising.

### **Strong Attribution For Identity-Linked Actions**

A holy grail of web advertising technology is a demand-centric attribution protocol with provable performance metrics. When advertisers pay for performance rather than impressions, it no longer matters whether an impression is a human or a bot; if the impression results in a purchase, the advertiser’s ultimate objective has been met.

In general, attribution for actions in web advertising is low-quality. It is very difficult to measure whether a product was purchased as the result of the purchaser having viewed advertisements unless the purchase happens in a click-through. Even then, it remains difficult to attribute credit for that purchase to advertisements for the same product the user may have viewed previously on different publisher sites. Advertisers simply do not know whether what they are doing really works, and publishers are disinclined to provide such information because it is more profitable for them to bill by eyeballs than by performance.

Cookie-syncing and all the black magic of adtech on the web has not produced a good attribution technology for the open web to-date. Open identity systems running on blockchains have the potential to

provide all the richness and assurance of data harvestable by closed social media platforms and finally provide the kernel of persistence necessary for strong attributions on the open web.

### **Advanced Voting and Governance Systems**

adToken holders are able to participate directly in voting on applications for listing in the adChain Registry. It will be desirable to empower adToken holders to safely delegate their votes to smart contracts like Gnosis prediction markets, or to trusted representatives in a similar vein to proof-of-work mining pool participation.

Another direction to explore is time-locking tokens used in voting, which has been discussed by Vitalik Buterin and others.<sup>10</sup> Time-locking tokens used in voting could increase voter stake in the adChain community beyond the tactical game of vote outcomes, because positions could only be exited over a strategic timeframe.

### **Impression Tracking**

Beyond facilitating discovery for peer-to-peer header bidding, adChain can also be extended to function as an accounting tool for near-realtime impression tracking. For traditional ad contracts with 30 to 60 day settlement cycles, discrepancies in impression reporting between parties are not discovered until the contract is complete. Discrepancies in tracked impressions commonly reach up to 20%.<sup>11</sup> Some of these are intrinsic to browsers and networks and come from latency, network connection errors, ad blockers, and differences between ad server spam filtering techniques. The widespread acceptance of discrepancies across the industry, however, is exploited through fraudulent tampering of metrics and misreporting impressions.

Using state channels, an advanced technique which allows for secure off-chain transactions that are instant, private, and cost zero gas, impression events can be synchronized between peers in real time, eliminating a category of fraud. The state channel implementation to track impressions has already been prototyped and the code and documentation is on GitHub here:

<https://github.com/adChain/AdMarket>. Once deployed, this will be the first production-ready state channel implementation, and it will be operating at web scale, with the ability to process billions of impressions per day, secured by smart contracts on Ethereum.

### **Micropayments and a True Three-Sided Advertising Market**

As described above, the first AdMarket implementation will primarily be used for accounting; the actual payments will happen out-of-band through traditional bank transfers. In time, the AdMarket state channel implementation will transition to a true micropayments system. In this system, advertisers will pay publishers tiny amounts on every cleared impression, to be settled periodically on-chain.

Through Ethereum wallet browser extensions such as MetaMask, users will also be able to participate in the market for their attention by automatically paying the publishers of the websites they visit the fair

---

<sup>10</sup> “[On Coin-lock voting, Futarchy and Optimal Decentralized Governance](#)”. Vitalik Buterin. Reddit. 2016.

<sup>11</sup> “[Third-party discrepancies](#)”. Google DoubleClick.

market value of their advertisements in order to respectfully block their ads. Further, if users choose not to block ads, publishers can choose to share their advertising earnings with them.

### **Real Time Data Streams**

The adChain protocols can be extended to facilitate discovery and purchase of real-time data streams of user engagement with advertisements for micropayments over state channels. This can either be sold by advertisers and publishers who capture this data or, in what would represent a paradigm shift, by users themselves. Users with Ethereum wallet browser extensions could capture and store their own data, and sell authenticated data streams linked to their identities (if they choose) to analytics providers, advertising retargeters and resellers, and other buyers.