XCHNG

BROUGHT TO YOU BY **KOCHAVA**

Contents

XCHNG ABSTRACT

Digital Advertising has been in existence since the first banner ads were published in 1994.[1] Over the next few years, a nascent industry became the primary means to engage with audiences digitally. Today, digital advertising has matured into a $224B global industry[2]; $83B in the U.S., of which $58B is in mobile.[3]

Countless advertisers, agencies, publishers, exchanges, ad networks, and affiliate networks drive the growth of the digital advertising industry. Today, its reach touches web, search, social, mobile, in-app, cross-device, and OTT (over the top) and is on the verge of grabbing hold of VR (virtual reality), AR (augmented reality), in-transportation, and ads delivered by your smart refrigerator. Because of the size of the industry, the supporting middleware has grown, serving as the "glue" that binds the disparate parts of digital advertising together (ad servers, mediation servers, fraud monitors, attribution and tag managers, creative managers, optimizers, and analytics providers, to name a few).

Despite its rapid growth, the scope of its reach, and the numerous actors transacting business within its ecosystem, the industry uses an antiquated paper-based contract framework called the Insertion Order (IO) which is rife with inefficiencies and does not provide a mechanized way to verify contractual commitments. Further, the plurality of secondary actors delivering on the terms of the IO, coupled with the absence of transparency across the industry, provides enormous opportunities for fraud through the delivery of the IO.

The industry has come a long way since the HotWired ads of 1994, but in many respects, it continues to operate in the past:

- No system exists which enables targeting audiences at scale while protecting the actual identity of the targeted audience devices. The absence of such a system has resulted in the industry's dependence on the advertising duopoly of Google and Facebook.
- 50¢ of every $1 is spent on middleware, mediation, and fraud mitigation.[4]
- Insertion Orders have no automated mechanism by which their terms are trafficked and verified.

U.S. digital advertising today is an $83B industry, $58B of which is in mobile.[3]

Kochava Labs SEZC is introducing the XCHNG platform to equip the digital advertising ecosystem with an open and unified blockchain framework a) facilitating the workflow of buying and selling ads through a smart contract IO; b) enabling the related matching and activation of audiences; c) bolstering ad-spend efficiency and security; d) adopting a next-generation advertising system of record for all ecosystem participants; and e) tokenizing the framework to treat digital ads as a true asset class.

[1] https://www.wired.com/2010/10/1027hotwired-banner-ads/

[2] https://www.emarketer.com/Report/Worldwide-Ad-Spending-eMarketer-Forecast-2017/2002019

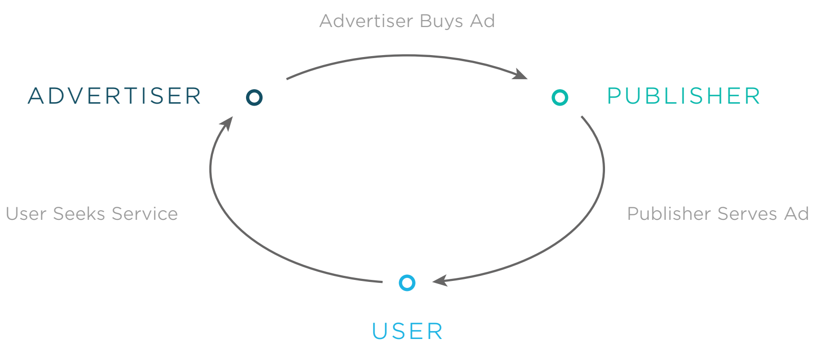
[3] https://www.emarketer.com/Report/US-Ad-Spending-eMarketer-Forecast-2017/2001998

[4] Arete Ad Tech Summary: Digital Ads: A Mad Market by Any Measure—May 22, 2017

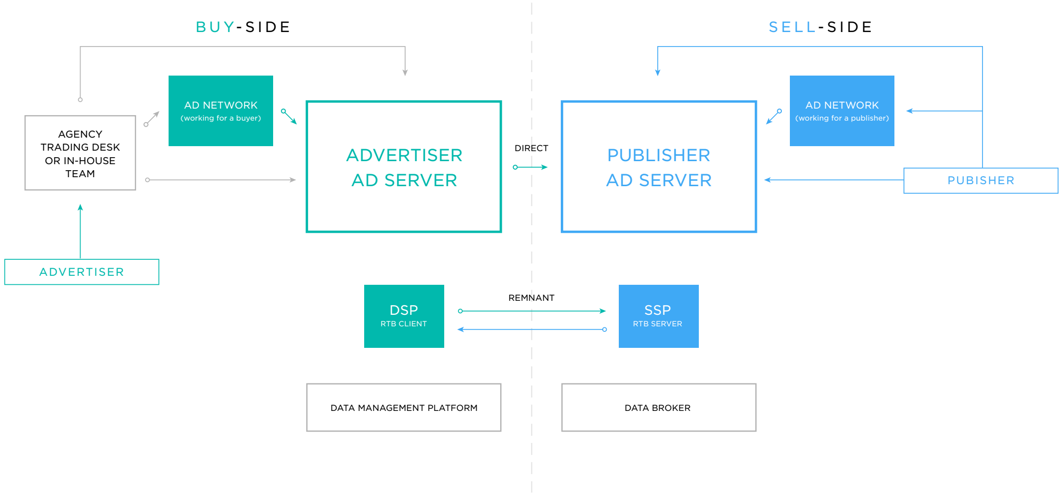
DIGITAL ADVERTISING TODAY

Overview

In its simplest form, digital advertising facilitates the delivery of marketing messages and content to consumers across the Internet, mobile apps, and other connected devices.



In reality, the process has become extremely complex, with many actors working together within this ecosystem under individual contractual agreements.



An example of how the digital advertising ecosystem works today

Buyers/Advertisers

Buyers or advertisers (also referred to as marketers), purchase media for the purpose of digitally advertising their apps, games, services, ideas, web sites, or products.

Publishers

A publisher (company or individual) is an entity who has a published website or app where it displays advertisements to its audience. These ads typically are provided by an advertiser in order to promote its products, services, or apps to the publisher's audience. The publisher provides a certain number of ad units within which the ad is displayed (banner, video, interstitial, content, or some other unique unit type). For the purpose of this white paper, we refer to an ad unit as an ad slot. A web page or app may have one or more portions corresponding to ad slots for displaying ads of various formats.

Aggregators

To support the scale of exposure required for a typical ad campaign (also called an "ad buy"), an advertiser is likely to engage with more than one publisher to achieve its campaign objective (i.e., access to enough ad slots). The advertiser may also engage with any number of ad networks (also called supply-side providers or SSPs) who aggregate ad slots from multiple publishers in order to provide the advertiser with greater scale to buy ad slots across a broader audience base. In a similar manner, a publisher with more than one ad slot may engage with more than one advertiser to fill its ad slots. Conversely, a publisher may engage with an advertiser aggregator (also called a demand-side provider or DSP) who aggregates advertisements from multiple advertisers to fill available ad slots. Furthermore, SSPs also interact with DSPs to provide even greater economies of scale. This system of aggregation is entirely centralized today.

Process

The administrative efforts required to negotiate and execute an IO according to its rules is a manual, tedious process. The involvement of third-party partners (SSPs and DSPs) driving scale further complicates the task. The process of buying or selling an ad slot requires the following elements:

- Executing an IO (the contract used to memorialize the transaction) for each campaign (or flight)
- Determining payment details
- Qualifying filtering and targeting criteria for the flight (establishing the audience characteristics against which the ad buy should correspond)
- In addition to the above, an advertiser often specifies supplementary terms, including:
  - Daily Pacing: Instead of displaying the advertisement in an ad slot all at once, the publisher displays the ad on a specified schedule
  - Fill Guarantee: The publisher fulfills the IO as a function of ad inventory volume

Pricing

Publishers and SSPs on one side, and advertisers and DSPs on the other rely on one-to-one negotiation to execute an IO. Historically, a rate sheet of the ad inventory value was established on a per source basis, but today, publishers and SSPs apply heavy discounts and premiums based on targeting criteria. These targeting criteria run the gamut: time of day, run of network versus site-specific targeting, geographic targeting, positioning of ad slot on web page or app, type of ad slot, supply of ad slots, demand for advertisements, etc.

The difficulty of placing an accurate market value on ad inventory adversely impacts both the demand-side and supply-side. Typical of true market dynamics, a publisher often underprices its inventory, whereas an advertiser constantly runs the risk of overpaying for its required inventory.

The advertiser typically pays a certain price for displaying its ad in an ad slot. Each placement of an advertisement or other digital content or media in an ad slot is referred to as an impression. Typically, an advertiser pays the publisher a price for each ad impression based on an expected return on investment (for example, a user of the web page or app purchases a product featured in the ad). Impressions that result in some form of action by a viewer of the ad are referred to as conversions. It should be noted that conversions are not limited to the purchase of a product. A conversion can also include the viewer clicking a hyperlink within the ad to access more information about the product.

As discussed above, a digital advertising marketplace can include both a supply-side economy, and a demand-side economy. The demand-side economy includes advertisers (or DSPs) that demand an inventory of impressions for placement of advertisements in the ad slots. The supply-side economy includes publishers (or SSPs) that provide an inventory of impressions for placement of advertisements in the ad slots. As the volume of publisher SSPs increases, there is a corresponding increase in the number of available impressions for advertisers or DSPs to purchase. In traditional markets, real-time bidding (RTB) may be used to sell available impressions to advertisers. One example implementation of an RTB framework is OpenRTB, described in detail in the OpenRTB API Specification Version 2.3.1, Interactive Advertising Bureau[5].

All RTB implementations, whether OpenRTB or not, use the same basic framework of a centralized, client-server bidding approach. RTB enables SSPs to acquire impression inventory from publishers and sell it to DSPs using a market-driven bidding approach. In this scenario, SSPs aggregate a supply of impressions, and DSPs aggregate demand for impressions for placement of ads. Together, the SSPs and DSPs enable an auction-style marketplace. Typically, an RTB environment is made up of each impression being bid on by multiple buyers (on a per-impression basis). The buyers are typically DSPs, although large advertisers may also gain access to the RTB market. Often, the RTB marketplace is set up to award the winning bid to the highest bidder at or just above the offer price of the second-highest bidder's offer. Finally, RTB is typically used as a final effort to sell inventory that is not already sold as premium inventory and is classified as remnant inventory.

> The complexity and innefficiency of today's digital advertising ecosystem, coupled with the dominance of the duopoly, make it ripe for a new paradigm.

RTB, and the roles that DSPs and SSPs play in the sale and purchase of impressions, could be considered as a means to overcome the challenges mentioned above. The problem with this approach is that there is still a centralized requirement whereby a particular DSP must be

[5] Interactive Advertising Bureau. "OpenRTB API Specification Version 2.3." Accessed July 7, 2017. https://www.iab.com/wp-content/uploads/2015/06/OpenRTB-API-Specification-Version-2-3.pdf.

connected to available SSPs. Similarly, for publishers to make their inventory available to buyers, their integrated SSP must be connected to DSPs that buy inventory from them. In most cases, an advertiser must still consult and work with multiple DSPs, which is complex, inefficient, costly, and time consuming. There is also a concern that by working with multiple DSPs, the advertiser may, in fact, be competing with itself if both DSPs from which the advertiser is buying are connected to the same SSPs. (In this case, the same advertiser is driving the cost up against itself via two separate DSPs).

DSPs may also take an IO and then buy directly with specific publishers. This may or may not be known by the advertiser. In the same way, the publisher receiving a sub-order may turn around and buy from another third-party publisher to fulfill the IO. This circumstance creates a re-brokering situation that is neither tracked nor accounted for in a true market-driven environment.

Finally, because RTB only makes inventory available in the immediate moment, there is no way to account for auction-based market dynamics for an ad buy set to occur in the future.

As the volume of available impressions continues to increase, advertisers, publishers, and underlying supply chains face increasing levels of complexity in managing demand and supply for impressions, ensuring that the available impressions are quickly and efficiently sold to advertisers for ad placement—and doing so in an open, distributed fashion.

As the volume of available impressions increases, advertisers, publishers, and the underlying supply chains face increasing levels of complexity.

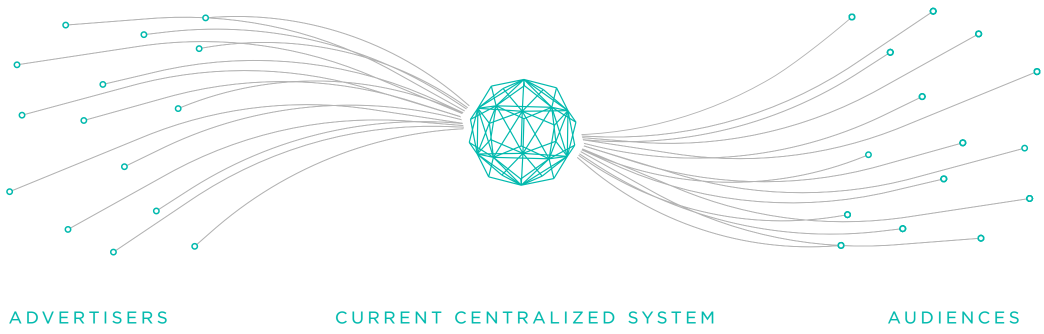
Measurement in Digital Advertising

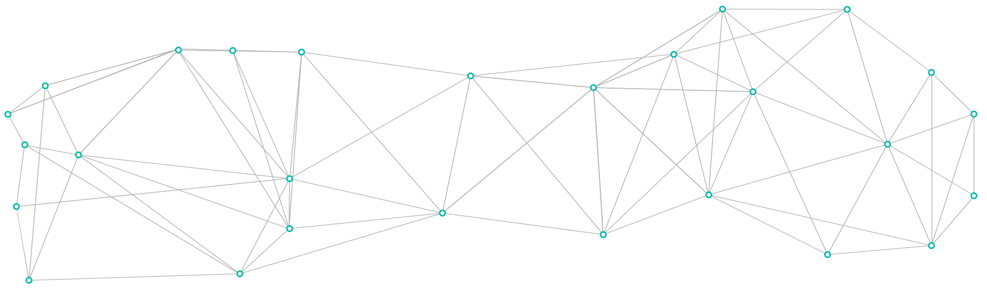
Measurement across the digital advertising ecosystem involves measuring impressions, clicks, key performance indicators (which may represent a conversion from a promoted effort) and assessing lifetime value (LTV) of the consumer and the source media to indicate if the advertiser should buy more of the noted inventory. Measurement is typically most trusted when independent from the advertiser and the publisher (a true independent third party) and, therefore, requires 1.) adoption by advertisers as a singular system of record and 2.) the trust of the inventory source publishers with which the measurement tool must integrate.

On the web, measurement has historically been done by tracking media efforts (impressions and clicks) and separately instrumenting pixels on a designated web property from which the key performance indicator (KPI) could be identified. In mobile, things are more complex and an integrated software development kit (SDK) is required to track mobile app KPIs. In the web 1.0 generation, DoubleClick became the predominant leader in measurement. Other stand-alone tools entered the market after Google acquired DoubleClick (Adometry and Convertro are two examples; both ventures have since been acquired).

DIGITAL ADVERTISING TOMORROW:
A Global Distributed Ledger Facilitating End-to-End Workflow

The need exists for an alternative technological approach that would facilitate the transaction of IOs via a crypto-based distributed ledger. This unifying and open approach would enable all parties that participate in the workflow of the IO to transact together. These actions start with discovery and negotiation and move through the lifecycle of execution, measurement, payment, and participant ratings.





OPEN DECENTRALIZED FRAMEWORK

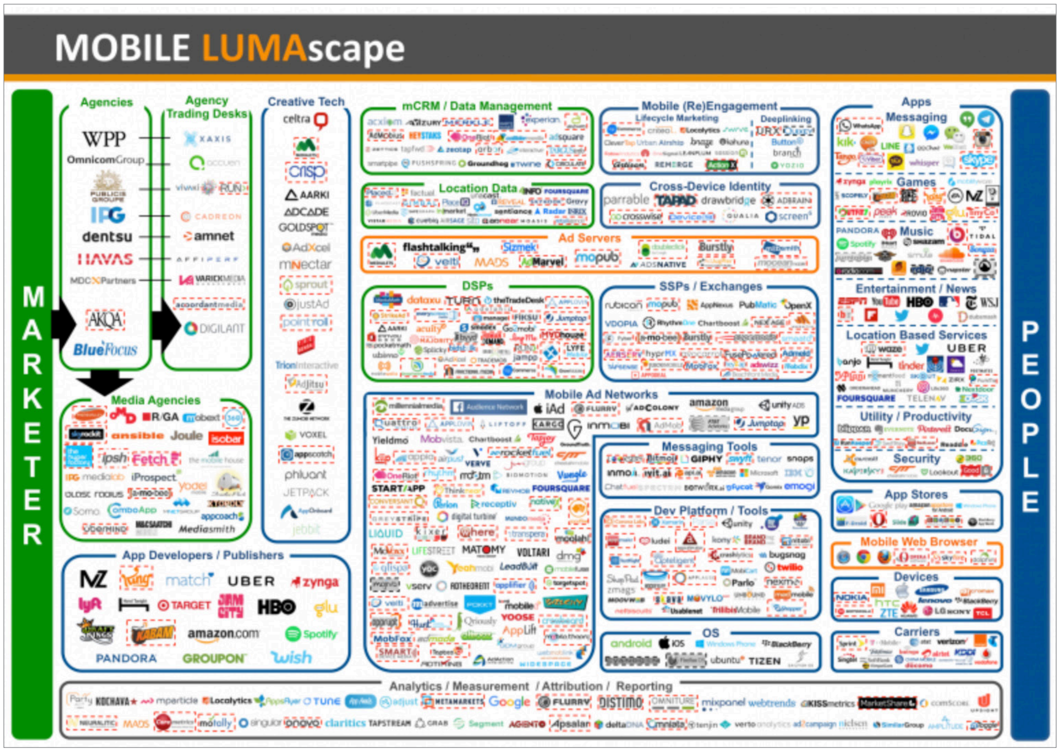
Kochava owns proprietary rights to such a system based on patents filed in 2015. The framework is centered around a common Ricardian contract with an open blockchain implementation called XCHNG that persists transactional history and provide supporting utilities required for maximizing efficiency through the lifecycle of the IO.

The framework enables a commercial entity (like Kochava Inc.) to attach its demonstrable leadership as a trusted system of record against an open blockchain implementation so that the ecosystem can unify and scale further. The system contemplates a next-generation blockchain implementation that handles the operational realities of digital advertising and supports the requisite components for the ecosystem to evolve from its current state. It is designed to provide participants with an easy roadmap to run on an open blockchain standard for digital advertising. While the status quo is a centralized exchange approach, the XCHNG framework is a decentralized approach.

While there have been several efforts that leverage blockchain-based protocols in digital advertising (e.g., adToken, Basic Attention Token, AdEx), none provide an end-to-end solution, and none are endorsed by a company with the reach and experience that Kochava Inc. has in the industry as a system of record. While there are ways each of these blockchain technologies may interface with XCHNG, it's important to note they are not attempting to accomplish what XCHNG proposes.

Digital advertising has reached a boiling point similar to other industries that have been overhauled in order to remain viable. Case in point: In the 19th century, the railroad industry was experiencing hypergrowth. Various independent companies formed their own rail networks, but details like the gauge of the rails were not initially standardized because they didn't anticipate the eventual interchange of equipment. Only once the rail networks were required to interconnect was there a profound observation that a common rail was critical to network transport at scale. At that time, the rail gauge debate evolved into regulated standards as the transport of goods was critical to national interests.

Similarly, digital advertising has grown from a single ad unit on HotWired in 1994 to a $224B worldwide industry today with a vast landscape of vendors that, when illustrated in one place, looks like an eye chart. The industry is confusing and splintered by value proposition, as demonstrated by the LUMAscape diagram below.



The XCHNG framework represents a common, open, and extensible set of "rails" on which companies like Kochava Inc. (as well as the participants shown in the diagram, above) can leverage blockchain in their commercial product offerings.

Kochava Inc. has committed to deploy XCHNG and be the first reference implementation of the XCHNG system, thereby providing the added benefit of on-boarding advertisers, publishers and all of the vendors within the value chain that already work with Kochava Inc. As highlighted by various players in the industry, achieving wide-scale adoption without a catalyst or support for existing tools to apply the technologies at scale is a great challenge.

The Digital Advertising Duopoly Runs its Own Markets; Causes Inefficiency; Represents Majority of Growth

Not everyone believes that an open rail framework is useful to the industry. Today, a duopoly exists comprised of Google and Facebook. The work performed by these companies to make advertising approachable, easy, and fluid to advertisers has been at the expense of being a truly open market. As such, it has also been at the expense of unifying the buyers and sellers—friction-free and efficiently. No doubt, their approach has been met with success. According to the Interactive Advertising Bureau (IAB), in Q1 2017, US advertising grew by $3.7B year over year. Facebook and Google represent 98% of this growth. Despite this success, it does not represent a true exchange with open, transparent, market-driven transactions.

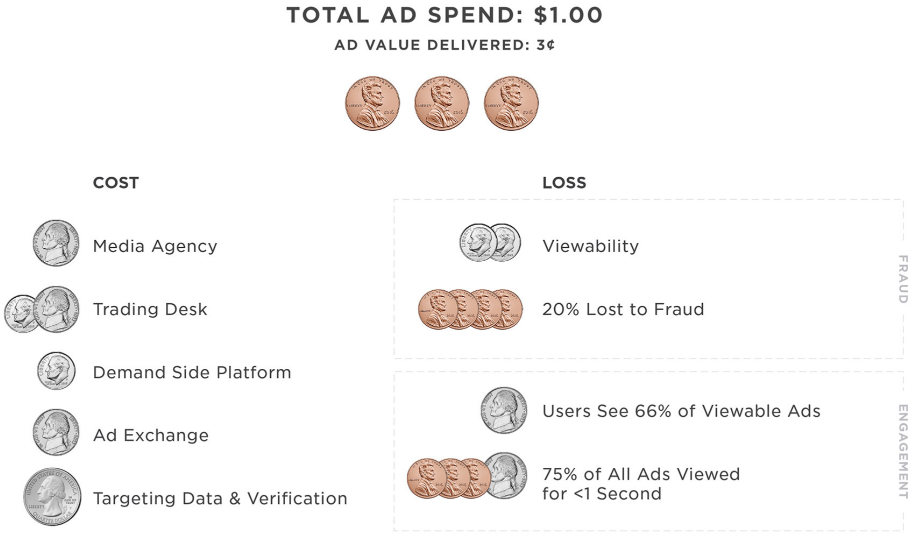
Using public equities as a reference example for a true open market, the following table shows how Google owns its market to extract more of the ad dollar and masquerade as an open market when it is not.

Exchange	Market Maker/IDB	Broker	Stock/Property
NYSE/LSE	Investment Banks	Banks, Schwab, eTrade, etc.	Individual Stocks, Composite Index, S&P 500, etc.
Google AdX (10% fee)	DoubleClick (20%)	DoubleClick for Publishers (20%)	Search, YouTube, Maps, AdMob Properties
Facebook Audience Manager/Atlas	Facebook Auction Engine/Atlas	Facebook Audience Network (FAN)	Facebook or FAN sites

Of a total digital advertising transaction value, Google extracts 30% to 50% in fees, plus captures the data in the supply chain while representing that it provides "market-based inventory availability" for advertisers. Nonetheless, Google carries a disproportionate market share because of the rules for integration. To cross-compare with the financial market, the following observations are clear:

- **Exchanges are not allowed to "make markets" in individual stocks/properties.** In the case of Google, it owns the pool of liquidity in its own properties and it supplements via third-party properties through AdMob. Facebook does the same with Facebook Audience Network (FAN).
- **Market makers are not allowed to provide liquidity in their own shares because it causes market manipulation.** As property owners, Google and Facebook see "both sides of the trade."
- **It is not a viable market condition to enable Google to be the only broker for YouTube (via DoubleClick).** Nonetheless, because of the strength in the associated platforms, both players set their own rules.

Outside of this duopoly, efficiency using independent actors is not more impressive (which is why the duopoly has been successful). This is because an advertiser must discover inventory, settle on terms, buy through various channels, ensure that the inventory is not fraudulent, and verify that delivery was performed. Further, they must also do all this at scale in order to be meaningful in the market and reach the most customers.



In the current digital advertising paradigm, ad spend is incredibly inefficient.

In the presence of the duopoly, independent media sources and ad networks desire to connect directly to the market demand.

Turning Digital Ads into an Asset Class

An asset class is a group of assets that have similar characteristics, behave similarly in the marketplace, and are subject to a common set of laws and regulations. The financial industry generally agrees there are three to five core institutional asset classes:[6]

- Securities (stocks)
- Bonds
- Property
- Commodities
- Cash (or cash equivalents)

As mentioned, the contract to bind a buyer and seller of a digital advertisement is typically in the form of an Insertion Order. To standardize terms in an IO, the Interactive Advertising Bureau (IAB) established standard IO templates for buyers and sellers to use to ensure fairness and clarity—the current version is 3.0.[7] The IO has always been paper-based (or electronic form of paper) and is the binding contract establishing that a publisher with inventory of ads will make them available to an advertiser who wants to buy the ads. With

[6] https://en.wikipedia.org/wiki/Alternative_asset

[7] https://www.iab.com/wp-content/uploads/2015/06/IAB_4As_tsandcs_Education_FINAL.pdf

the splintering of participants in the value chain, arbitrage and re-brokering have become commonplace using the commitments of media buys as the basis for the asset that is being traded.

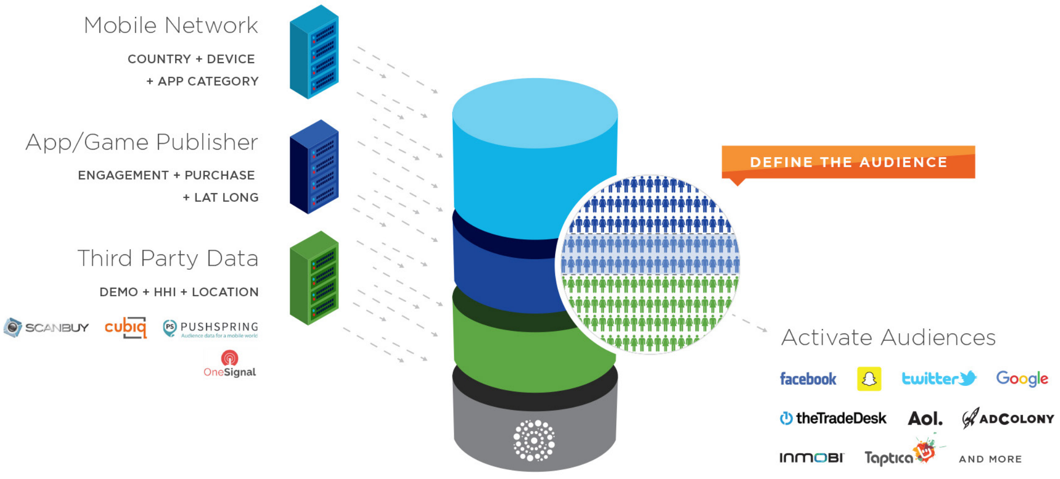
Despite the reality that agency trading desks, exchanges, and ad networks behave as if advertising inventory is bought, sold, and traded, the reality is that none of it is mechanized in a way that can be scaled. It is rarely verifiable at scale as an asset class, integration across the system is terribly inefficient, and there is no common denominator mechanism to provide liquidity.

> A true asset class would provide for standardized, fully integrated, and verifiable digital ad inventory with a common liquidity framework.

Equities, bonds, property, commodities, and cash are the most liquid asset classes and therefore, the most quoted asset classes. There are also alternative asset classes such as real estate, artwork, and collectibles. The more alternative the investment, in general, the less liquid. In its current state, a purchased IO between buyer and publisher is illiquid and deemed a service delivered (i.e., an ad shown to a publisher's audience). Treating digital ads as a true asset class would mean providing standardized, fully integrated and verifiable digital ad inventory with a common liquidity framework.

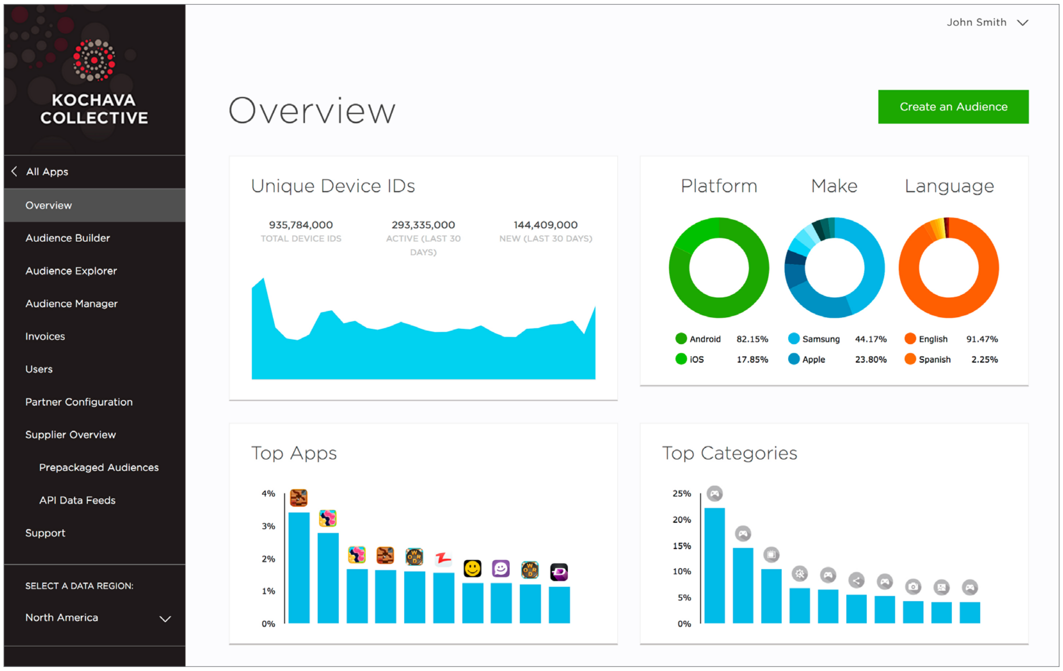
Facilitating Open Audience Targeting Across Media Sources

In September 2015, Kochava Inc. created a new targeting platform for mobile audiences called the Kochava Collective. The basis of the Kochava Collective was to provide a unified audience graph that would enable advertisers to query and target audiences with device-level precision for their advertising campaigns. Based on this targeting, the centralized system would enable distributed activation in a de-duplicated way to best address (i.e., serve ads to) the audiences identified through the targeting process.

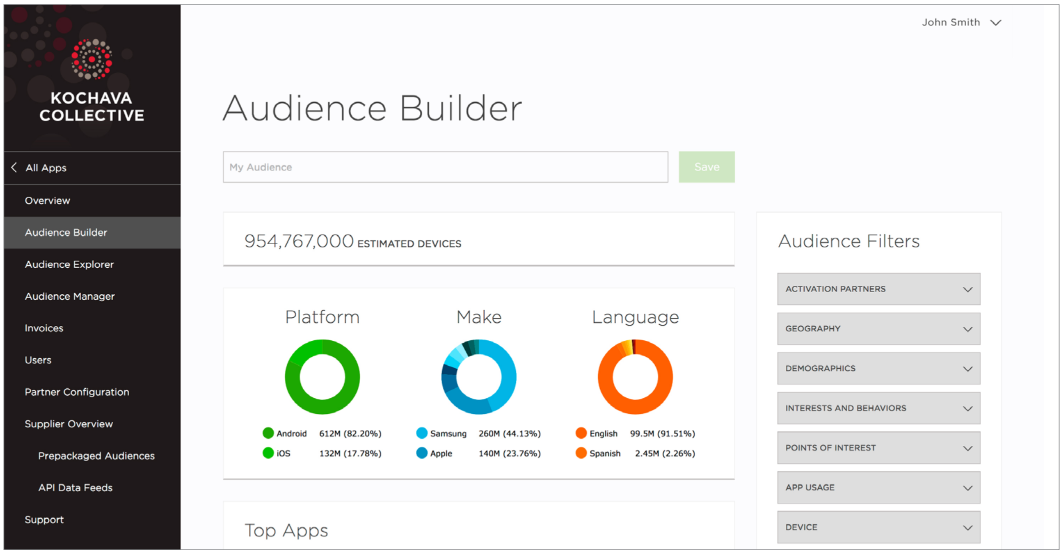


KOCHAVA COLLECTIVE

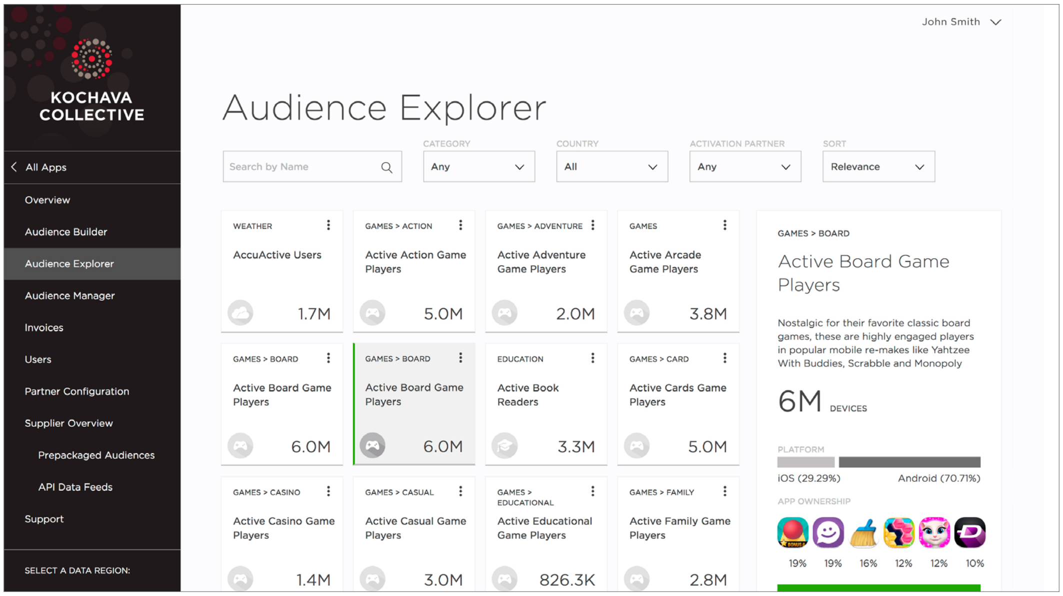
Today, the Kochava Collective is a centralized database of mobile devices. When Kochava Inc. introduced the Kochava Collective, it had its eyes on building a blockchain-backed system of record for all of digital advertising and recognized that the value of the chain would be directly related to an advertiser's ability to browse the chain for the audiences they would want to target.



An example customer Overview screen in the Kochava Collective



Customers can build custom audiences or browse pre-defined audiences that match their criteria in the Kochava Collective.



Audience Explorer

Search by Name
CATEGORY: Any
COUNTRY: All
ACTIVATION PARTNER: Any
SORT: Relevance

WEATHER
AccuActive Users
1.7M

GAMES > ACTION
Active Action Game Players
5.0M

GAMES > ADVENTURE
Active Adventure Game Players
2.0M

GAMES
Active Arcade Game Players
3.8M

GAMES > BOARD
Active Board Game Players
6.0M

GAMES > BOARD
Active Board Game Players
6.0M

EDUCATION
Active Book Readers
3.3M

GAMES > CARD
Active Cards Game Players
5.0M

GAMES > CASINO
Active Casino Game Players
1.4M

GAMES > CASUAL
Active Casual Game Players
3.0M

GAMES > EDUCATIONAL
Active Educational Game Players
826.3K

GAMES > FAMILY
Active Family Game Players
2.8M

GAMES > BOARD
Active Board Game Players

Nostalgic for their favorite classic board games, these are highly engaged players in popular mobile re-makes like Yahtzee With Buddies, Scrabble and Monopoly

6M DEVICES

PLATFORM
iOS (29.29%) Android (70.71%)

APP OWNERSHIP
19% 19% 16% 12% 12% 10%

Pre-defined audiences are searchable by category, geo, and activation partner.

The Kochava Collective has already experienced significant traction, becoming the largest independent mobile data marketplace in the world (1.8B unique device profiles at the time of publication). No other tool outside of those provided by Google or Facebook offer targeting abilities against mobile devices at the same scale and precision. Integration of the Kochava Collective on the XCHNG blockchain provides a significant and unique opportunity to advertisers.

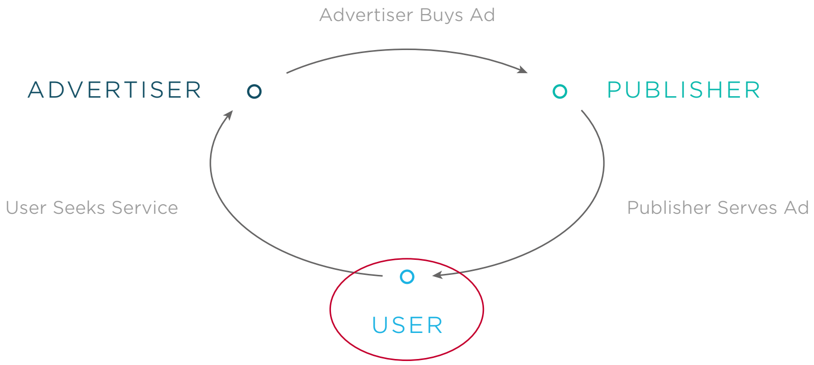
In addition to providing advertisers with the arbitrary ability to query audiences, the Kochava Collective provides pre-defined segments that cater to advertisers' selection interests.

While the Kochava Collective has been built as a centralized system to date, it will be equipped to enrich the data introduced by the publisher inputs on the XCHNG distributed system upon launch of XCHNG.

This approach, while making competition an open opportunity for others against the Kochava Collective, enables wide-scale adoption across the industry for XCHNG. Upon launch, the Kochava Collective will be a first reference implementation of targeting tools using the XCHNG system and an elegant industry competitive user interface to discover and browse the audiences that are targeted and activated against on XCHNG.

Enabling a Role for End Users in the Value Exchange in Digital Advertising

While the value chain of advertising includes advertisers, publishers and end users, often the end user is left out. Many argue that end users desire better interest matching (or targeting) so the right offer can be made available to them, and advertising could work to their benefit.



XCHNG creates a way for end users to submit interest-matching criteria for use when advertisers are targeting audiences. Not unlike the virtuous cycle on Facebook, where end users fill out their interests, demonstrate engagement through posts, and self-identify friends, all of which Facebook uses as targeting criteria for advertisers, the XCHNG framework enables users to get value out of their matching (targeting) criteria.

THE XCHNG TOKEN AND PROPOSAL FOR THE FUTURE

Kochava has designed and developed an open, crypto-based ledger framework that is the manifestation of a smart contract system for advertising. Unlike the paper-based version of the contract to buy and sell digital ads, the smart contract IO codifies all the elements of a well-formed IO into a fully traceable and immutable electronic Ricardian contract, binding the following key elements:

1. Identification and pre-verification of inventory being bought, sold, or traded with associated targeting capabilities against an open blockchain framework
2. Identification and pre-verification of the Buyer and Seller of the media with unique keys
3. Embedded and programmable terms for the agreement that address traffic and brand safety verification, targeting (from 1, above), allowance of re-brokering, flight times, payment approach: CPM (Cost per Mille—impression-based pricing), CPC (Cost per Click), CPI (Cost per Install), CPX/CPA (Cost per Action) and other details for the digital ad buy; General Data Protection Regulation (GDPR) compliance
4. Identification of the associated ecosystem partner to be used for the purpose of measuring performance of IO terms (called the Measurement Provider)
5. Identification of the optionally associated ecosystem partner to be used as the Ratings Provider
6. Identification of the optionally associated ecosystem partner to be used as the Payment Provider (For clarity, Kochava will not serve in this capacity on XCHNG).
7. Identification of the optionally associated ecosystem partner to be used as the Arbitration Service in the event there is disagreement between the Buyer, Seller or Measurement Provider upon delivery

By codifying the IO into a smart contract written to the XCHNG distributed ledger, the associated inventory is effectively an asset class, replete with a) traceable history, b) capacity for delivery verification, c) arbitrage opportunity and, most importantly, d) liquidity.

XCHNG: The Blockchain for the Advertising Industry

Key elements have materialized, which enable the tokenization of an IO with the supporting immutable infrastructure to facilitate various actors in advertising to commercially participate.

The XCHNG system is a global distributed ledger that facilitates Buyers and Sellers to transact with Measurement Providers, Ratings Providers, and Payment Providers to participate in the smart contract. The XCHNG system provides technological methods to both differentiate the XCHNG system and enable faster growth of the system as a whole across various verticals. Some of those differentiating features include:

- Daily rolling chains
- Incentive framework to motivate inventory addressability
- Crypto-based activation; protecting identity while publishing addressable identities openly
- A federated and open framework for market makers

Daily Rolling Chains

Blockchain-related technologies focus on the intrinsic value of openness and transparency, often pointing to a full historical record of all transactions recorded on the chain as a basis behind both immutability and anonymized transparency. While this is certainly valuable, there are many situations where the knowledge of transactional history is a competitive advantage for a participating company. For example, Buyers may not want transactional buying history available at large (despite being anonymized by a crypto key representing an actor). Further, a full historical chain of all transactions can create an unnecessary burden on participating nodes in the chain because of the architecture to include all transactions since day one. Indeed, in some industries (like digital advertising), the volume of transactions make the standard of storing every transaction on the chain a burden and not a benefit.

The Daily Rolling Chain differentiates XCHNG and addresses the challenge of transaction volume.

For these reasons, the XCHNG system features a Daily Rolling Chain (DRC). This is a key feature and differentiator of the XCHNG blockchain. The premise is that each node on the network only persists and can only validate a daily transaction history for those open contracts for a given day's date and moving forward in time.

Any contracts on the chain that represent completed flights would no longer be synchronized despite their existence having an impact on the overall chain signature. In summary, each day would represent day one of the chain with the originating block being the last consenus block from the previous day of transactions, with checks for chain validation at the time of the roll-over according to sufficient ratings status of those nodes participating in the consensus.

While any node can store historical data, the premise of the system's architecture is that no node is responsible for anything outside of the time boundary of a day. Key innovations have been developed to enable the approach of the DRC while ensuring trust for particular nodes using the ratings system of the chain so that new nodes can synchronize their daily chain with the confidence that what they are synchronizing is a true and correct version.

While the DRC is the architecture for the open system, key vendors in the supply chain are able to store each day's transactions cumulatively, as appropriate, to ensure the commercial service they're providing for the ecosystem. As a reference example, a Measurement Provider like Kochava Inc. would store more than a single day's worth of transactions as a Measurement Provider service.

While anyone could "listen" to the chain and store everything in entirety over time, our belief is that only those companies providing a service will do so. Consequently, those not providing a service will not. Further, historical data that vendors haven't observed prior to listening to the chain will suffer the consequences of being "late to market" in comparison to vendors who have adopted early. This provides embedded value to those companies that adopt the XCHNG system early for the service they plan to deliver to the ecosystem and does not benefit those that are late. This creates incentives for new ancillary players to store the full historical chain as a service to new entrants on the XCHNG system.

In conclusion, while manifesting transaction history on the open blockchain system of XCHNG delivers appropriate transparency and openness, the system has been architected to avoid the unnecessary burden of extraneous nodes on the system and to maximize scale for high-transaction volume applications like advertising.

Peer-to-Peer Network

The XCHNG network is a distributed network that consists of a peer-to-peer (P2P) transport layer. A distributed network can be considered a P2P network if the network participants share a part of their own hardware resources (for example, processing power, storage, network bandwidth etc.) Each network participant or peer is accessible by other peers directly, without passing intermediary entities.

Peer Membership List

Distributed systems are made up of a group of nodes that need to communicate by sending messages between one another. In order for peers to communicate effectively, they must be able to identify their peers in the network. It is typical for each peer node to maintain a list of peers that they can reach in the network. The overall complexity of maintaining this list increases as peers join the network. Membership protocols have been developed to help track peer nodes in the network. Some membership protocols rely on sending "empty heartbeat messages" to each peer in a peer list in order to validate that the peer node is "alive." For example:

```
n = a remote node
t = random epoch time
for t
 r = send(heartbeat,n)
  if r != nil
    n = alive
  else
    n = dead
```

After a certain time period, if a peer node does not receive a heartbeat from another peer in the network, then the node is assumed to be dead. This is acceptable for a small cluster; however, as the network grows, the number of heartbeat messages sent to each peer in the list increases dramatically. Heartbeat protocols solve two separate problems: node failures and the need to maintain a list of active peers in the network.

To solve the network constraints associated with P2P, gossip-based membership dissemination protocols have emerged. These protocols work to reduce the number of heartbeat messages sent by each peer node. Each peer is required to forward messages to a set of randomly chosen peers in the network, instead of sending messages directly to every peer in the membership list. Approaches, such as the Scalable Weakly-Consistent Infection-style Process Group Membership or SWIM[8] allows for a weakly-consistent view of the peers in the network. This means that a given peer's membership list will eventually converge to the same state as other peer nodes in the network. The SWIM approach is made up of two components: a Failure Detector and a Dissemination Component. Failure detection is done by randomly probing peer nodes: If the peer node fails to acknowledge the message within a given time window, an indirect probe is attempted. An indirect probe selects a number of random peer nodes to probe the node in question. Indirect probes can be used to circumvent a network issue that caused the original node to fail the probe. If the indirect probe fails, then the target node is marked as "suspect." Peer nodes that have been marked suspect remain a member of the cluster for a set period of time. If the peer node is unable to dispute the suspicions of the network then it is eventually removed. Upon detecting a peer failure, the peer node simply broadcasts a failure message to the rest of the active peers. The peers that receive this failure message then remove the failed peer from their membership list. The process of sending out membership messages makes up the Dissemination Component.

Furthermore, approaches like Kademlia[9] use distributed hash tables to store peer nodes in the network. Kademlia peer nodes communicate with one another using User Data Protocol (UDP). A node ID can identify each peer node. The Kademlia algorithm works to find the closest node when a lookup is performed, contacting only O (log (n)) out of n nodes in the system. The distance between nodes is computed as the XOR of two node IDs. The Kademlia protocol consists of four remote procedure calls (RPCs): ping, store, find_node and find_value. The ping RPC sends a probe to a peer node to see if it is online. The store RPC tells a peer node to store a key value pair for later retrieval. The find_node RPC returns the IP address, UDP port, and node ID for the key provided. Find_value works similar to the find_node RPC, with the exception that if a store RPC has been issued for the ID in question, then the value stored is returned.

Peers in the XCHNG P2P network utilize similar protocols. Strategies similar to the approaches above are being tested within XCHNG for performance, consistency, and fault tolerance. Our goal is to have a reliable, scalable, and fault-tolerant membership protocol that can be used by our P2P transport layer when communicating with peers in the network.

Message Broadcasting

Peers broadcast messages by selecting peers from their membership list. The P2P transport layer is only responsible for the delivery of messages. However, additional metric support, such as, Round Trip Times (RTT), Node Health, and other common metrics are added to aid in successful delivery. The transport layer uses bidirectional streaming over transmission control protocol (TCP) to send messages efficiently to other remote peer nodes. Each peer holds a membership list of remote peers. When a message is sent to a peer, they begin to broadcast to their remote peers.

[8] https://www.cs.cornell.edu/~asdas/research/dsn02-swim.pdf

[9] https://pdos.csail.mit.edu/~petar/papers/maymounkov-kademlia-lncs.pdf

Incentives

To be successful, the XCHNG system must operate like the enabling technology stack for other trading platforms, incentivizing both supply and demand to participate on the system. Demand on a trading platform is not generated unless there is a valuable supply. Equally, suppiers will not be motivated to make their inventory available unless there is a promise of demand.

For Buyers, the incentive of efficiency, the promise of inventory volume, and transactional transparency is sufficient incentive to buy (provided that the workflow is relatively friction free). The need exists to produce incentive for Sellers (publishers) to make inventory available on the chain and further for data providers to publish data about XCHNG-approved inventory so it can be targeted properly.

On the XCHNG system, miners can mine blocks on the chain to enable quality and quantity of inventory available for Buyers. In addition, in order to incentivize a healthy, reflexive ecosystem, miners can write ratings blocks about transactions found on the chain. The ratings are used as metadata about the participants on the chain.

The XCHNG system will include an incentive framework to motivate supply and data partners to make inventory available on the chain. The framework will likely be based on the following logic:

- Any node can introduce inventory of addressable audiences onto XCHNG as non-validated inventory. Addressable inventory is inventory that represents the ability to serve an ad to the specified device in the block. Included in the non-validated inventory is an addressable identifier used by the addressable media source (cookie ID, IDFA, ADID) against which the ad must be delivered if referenced in a resulting smart contract IO. The identifier is hashed using the key of the node introducing the inventory, thereby making the end user's advertising identifier private and only usable for delivering ads by the node that introduced the inventory.
- Any node can introduce metadata about addressable audiences onto XCHNG as non-validated inventory. Metadata includes, but is not limited to, device characteristics, apps running on the device, geographic location data, or other data that could be used for targeting. The primary key for the metadata is the device identifier (hashed with the key of the provider).
- A Measurement Provider writes transactions back to the smart contract IO, validating the inventory introduced by the provider.

Additionally, miners in the XCHNG system may earn tokens for generating new blocks. These blocks consist of transactions produced from a smart contract IO.

Inventory Publishing & Audience Activation via Crypto Keys

As previously mentioned, publishers on XCHNG make their inventory available as non-verified transactions onto the chain. The actual advertising device identifier is never published openly—all identifiers are hashed by the publishing node key. When Buyers target audiences in a resulting smart contract IO on XCHNG, the targeted device identifiers are not included in the payload of the contract. Instead, what is targeted is either non-specific device targeting data or, in the case of device targeting, a non-validated inventory or a validated inventory. This association means that publishers know which devices to target in an IO that they have signed on XCHNG, and no other node will know the identity of the device in the IO.

In concert with the community, the XCHNG system will have open implementations of ad servers and mediation servers which automatically publish inventory onto the chain and automatically rendezvous impressions with active IOs (and related hashed identifiers) to make adoption easier for publishers. Further, the XCHNG system will have a series of open plugin technologies enabling publishers using commonly used ad server technologies for digital ads (for example, DoubleClick for Publishers, or DFP) to take advantage of the demand being generated on the XCHNG system.

Federated and Open Facility for Market Makers

While the XCHNG system has been optimized for Buyers and Sellers to conduct directly on buying and selling inventory, we believe that an important role exists in advertising today which closely resembles that of a market maker in the equities market.

In the equities market, market makers compete for customer order flows by displaying buy and sell quotations for a guaranteed number of shares. The difference between the price at which a market maker is willing to buy a security and the price at which the firm is willing to sell it is called the market maker spread. Because each market maker can either buy or sell a stock at any given time, the spread represents the market maker's profit on each trade. Once an order is received, the market maker immediately sells from its own inventory or seeks an offsetting order. There can be several market makers for a particular stock, depending on the average daily volume. The market makers play an important role in the secondary market as catalysts, particularly for enhancing stock liquidity and, therefore, for promoting long-term growth in the market.

In the same way, the XCHNG system enables a means for federated market makers. Instead of making shares of equity available for buying/selling, the market maker manages various properties on which ads are delivered.

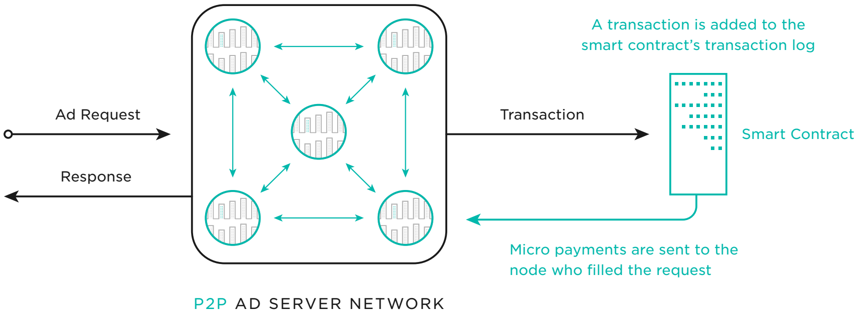
Decentralized Ad Serving Miners

The XCHNG system gossips[10] smart contract IOs to a P2P network of ad serving miners. Ad serving miners work to fill Insertion Orders by offering their network bandwidth and system resources.

Miners receive requests from clients and work to fill the response. Upon successful delivery, clients send back a receipt to the miners. Miners send their receipts back to the XCHNG system IO to receive a transactional payment. Miners are elected based heavily on their response latency to the request. However, it is also possible for an ad serving miner to be signed in directly to the IO. If a miner is unable to respond to the client, then traditional ad technology stacks can be used to fill the request.

[10] https://en.wikipedia.org/wiki/Gossip_protocol

AD SERVING MINERS


Ad Request
Response
Transaction
A transaction is added to the smart contract's transaction log
Smart Contract
Micro payments are sent to the node who filled the request
P2P AD SERVER NETWORK

In distributed systems, the CAP theorem states that is it is impossible for a system to achieve all of the following:

- Consistency
- Availability
- Partition Tolerance

Therefore, ad serving miners are designed to favor consistency and availability when answering requests sent by clients in the XCHNG market.

Consensus Model

Distributed consensus is a well-known topic when dealing with distributed systems. While it can be perceived to be complex, consensus can be simply defined as ***the process of agreeing on one resulting value among a group of participants.*** If no value is proposed, then no value should be chosen. If a value is proposed and chosen by a peer, then other peers should be able to learn the chosen value. Consensus is especially important in a distributed network of unreliable peers. Example consensus models commonly used with state-machine replication include protocols such as Raft[11] or Paxos[12]. However, additional consensus models are being implemented and tested by blockchain platforms. These include Proof of work, Proof of Stake, and Byzantine Fault Tolerance variants.

Proof of Work

Proof of work (PoW) originally provided an economic measure to deter denial-of-service (DoS) attacks against a service. PoW is more popularly known in the Bitcoin mining algorithm. Bitcoin uses the Hashcash[13] PoW algorithm, which requires a configurable amount of work to compute. A block in Bitcoin contains nonces (arbitrary numbers that can only be used once, in a 32-bit field set so that the hash of the block will contain a run of leading zeros) that a miner (node working to add a block) must set in such a way that the hash of the block is smaller than some known target. The amount of compute power needed to calculate the value is expensive. However, once the value has been found, it can be easily verified. The time it takes to generate a new block is known as block frequency.

[11] https://raft.github.io/raft.pdf

[12] https://lamport.azurewebsites.net/pubs/paxos-simple.pdf

[13] http://www.hashcash.org/papers/hashcash.pdf

Proof of Stake

There are few variants of Proof of Stake (PoS) consensus models today. However, it can briefly be defined as a consensus protocol that gives entities, which hold stake in a system, the ability to maintain the history of a distributed ledger. Stakeholders possess a fraction of the total amount of currency in circulation making them eligible to create the next block in the ledger. A stakeholder risks losing a fraction of their overall stake in the network if the security begin to degrade. Typically, PoS implementations are made up of validator nodes, which are randomly assigned the right to propose new blocks. Once a validator node is chosen to propose a block, multiple voting rounds take place. Other validator nodes send in votes for a specific block during each voting round. After the voting rounds, all validator nodes reach an agreement on which block to add to the blockchain.

Byzantine Fault Tolerance

A Byzantine fault can be described as any fault presenting different symptoms to different observers. Furthermore, a Byzantine failure is the loss of a system or service due to a Byzantine fault within a system that requires consensus. Byzantine fault tolerance (BFT) refers to a system's ability to defend against Byzantine failures. Byzantine broadly refers to the "Byzantine Generals Problem."[14] An interesting solution that is able to tolerate Byzantine faults is Practical Byzantine Fault Tolerance (PBFT).[15] PBFT uses three phases to each agreement: pre-prepare, prepare, and commit. The pre-prepare and prepare phases are used to totally order requests being sent to a peer in the network. Additionally, prepare and commit phases are used to ensure requests that are committed are totally ordered across all views.

XCHNG Consensus

XCHNG has been developed for a modular consensus mechanism. It is trivial to run different consensus models, such as, PBFT, Raft, Paxos, PoS, PoW, or hybrid solutions. Our first approach is a BFT solution that can be further enhanced by PoS. Similar to other PoS models, our consensus model consists of a set of validator nodes. The amount of voting power a validator node holds is based on the amount of state in the network. Voting for consensus on a transaction or group of transactions is done in rounds similar to the models above. Validator nodes can propose, validate, prepare and commit new transactions. When consensus is reached, validator nodes broadcast the transactions to the other peer nodes using our P2P network protocol. Ratings providers monitor validator nodes. If a validator node drops below a certain rating, it will be removed from the network. Anyone with stake in the network can become a validator node. However, due to communication overhead, there may be a limit on the number of validators.

Miners participate in the creation of new blocks. A PoS consensus model is used to determine the amount of voting power an individual miner has over the next block being generated. The more stake a miner has in the XCHNG network, the more voting power they hold. A miner's stake acts as a security and increases the loyalty of the miner.

PoS reduces wasteful energy spend that would otherwise be necessary in a Proof of Work consensus model. Additionally, the need for high-end or custom hardware to compete against other miners is not necessary. Lowering the barrier of entry to simply participating in the network.

[14] http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.126.9525&rep=rep1&type=pdf

[15] http://pmg.csail.mit.edu/papers/osdi99.pdf

Cross-Chain Communication

As the blockchain ecosystem continues to grow, more implementations pop up as viable solutions to the unique challenges blockchain systems face today. In order to adapt along with advancements in technology, XCHNG is designed to engage in cross-chain communication. This allows XCHNG to communicate with other blockchain implementations. Additionally, it enables XCHNG to interact with other decentralized applications that exists in the market today.

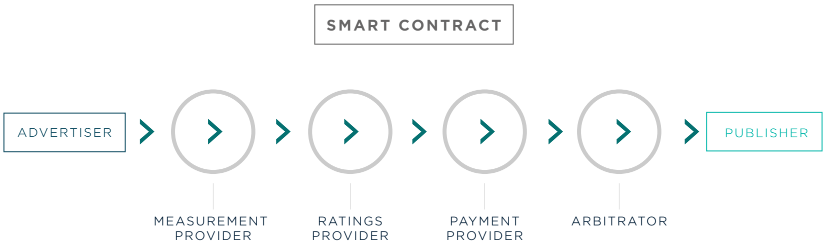
First-Party User Data

XCHNG is focused on increasing the value of publisher inventory, including audience metadata. In addition to traditional data management platforms, users have the ability to introduce data to the XCHNG market.

User data is stored on user devices. Publishers and advertisers do not have the ability to view user data directly. However, when a user publishes data to XCHNG, it can be added to a publisher's inventory. Advertisers can target user data using the same market protocols listed above.

Enumerating the Actors of Any Transaction in XCHNG

The following are the core actors in any smart contract IO within the XCHNG system. The only required actors for any transaction are the Buyer and Seller. The additional actors in the core named set enable market efficiency and accountability.



The smart contract codifies the transaction between an advertiser (Buyer) and publisher (Seller) including all terms and actions that have been designated to be included in the transaction.

Buyer

The Buyer is engaging in a contract to buy media. In digital advertising, a Buyer could also behave as a Seller, but for a singular contract instance, there is only one Buyer.

Seller

The Seller is engaging in a contract to sell media. In digital advertising, a Seller could also behave as a Buyer, but for a singular contract instance, there is only one Seller.

Terms (non-actor)

While the Terms are not an actor, they are the encoded directives that make up the terms of the agreement between Buyer and Seller. Terms include pacing, targeting, minimums, price, and pricing approach (to name a few).

Measurement Provider

The Measurement Provider can validate a contract between the Buyer and Seller given the context of the terms. Within the digital advertising context, a Measurement Provider must support the terms outlined programmatically in the agreement (such as pacing, day parting, or frequency capping of ad impressions). For example, Kochava Inc. is uniquely positioned to be a leading Measurement Provider on the XCHNG system. Because XCHNG is open, there is nothing stopping others from becoming Measurement Providers on XCHNG. Market dynamics should drive the best vendor in this or other roles.

The Measurement Provider role is optional in an XCHNG smart contract. If designated, the specified Measurement Provider for a smart contract is signed into the contract along with the terms.

Ratings Provider

The Ratings Provider is critical to the health of the XCHNG ecosystem as it provides ratings for all participants across all historical transaction history. This is particularly valuable when the chain of the XCHNG system is a daily rolling chain. Ratings Providers could provide ratings of inventory, ratings of advertisers, ratings for Measurement Providers or Payment Providers, or any other index that the market drives.

The Ratings Provider role is optional in an XCHNG smart contract. If designated, the specified Ratings Provider for a smart contract is predetermined and signed into the contract along with the terms up front. We believe that passive Ratings Providers will enter to serve the market, but they will be relegated to public data on the chain and not the key information that is not published on the chain.

The XCHNG blockchain has a role for basic ratings performed by miners to set public ratings of nodes on the network. While this free (and basic) ratings framework exists, we believe that commercial ratings vendors will still have a role for more detailed ratings capabilities signed into each IO.

Payment Provider

The Payment Provider is critical to support payment for agreed and executed smart contracts. The Payment Provider will conform to the payment terms outlined in the smart contract and release funds based on milestone release points outlined in the terms between the Buyer and Seller and based on Measurement Provider confirmation. Although the Payment Provider is optional in an XCHNG smart contract, we believe the XCHNG system will usher in a greater value to the Payment Provider to handle the complexity of billing and collections in digital advertising. Finally, a participating Measurement Provider is required if escrow service (from the Payment Provider) is designated, as there is no ability to release payment against a contract without a Measurement Provider playing a role in the smart contract. Like the other optional roles, if designated, the specified Payment Provider for a smart contract is predetermined and signed into the contract along with the terms up front. One particular class of company that is likely to find value as a Payment Provider is the factor-based payment vendors who will be able to provide accelerated payment to publishers for a fee. For clarity, Kochava Inc. does not participate as a Payment Provider.

Arbitrator

The optional Arbitrator role is designated in conjunction with the Measurement Provider and Payment Provider. If a dispute arises between Buyer and Seller (only if a Measurement Provider is designated), the Arbitrator is designated to handle the dispute. The legally binding terms of the designated Arbitrator will be agreed to when electing to designate a specified Arbitrator for a smart contract.

THE XCHNG ARCHITECTURE

The XCHNG system is unique in that the architecture is specifically outlined to support the named actors as well as the possibility of other actors not originally contemplated. Further, the Kochava team has built the technology platform as an open system. At the heart of the XCHNG architecture is a ricardian smart contract for transacting between Buyers and Sellers.

Smart Contracts

A smart contract is software being executed on a blockchain that defines the transaction instructions for an asset. Smart contracts handle the business logic agreed upon by members participating on the XCHNG network. Ledger state is scoped to the smart contract and is unable to be accessed freely by other smart contracts. However, access permissions can be given to another smart contract in order to access transaction state. The XCHNG API implements a set of standard interfaces that smart contracts must implement in order for them to be considered valid.

Smart Contract Lifecycle

The XCHNG API allows a user to sign, deploy, initialize and upgrade smart contracts that exist on the network. Additional functionality is being developed to make the smart contracts lifecycle more robust and manageable by end users. An Owner or Owners sign smart contracts. All operations run against a signed smart contract must be verified. Once a smart contract has been signed it can be deployed to the network through the XCHNG API. Once deployed, Owners of the smart contract can send additional commands to the XCHNG network via the API, such as initialize or upgrade. After the smart contract as been initialized, it can begin processing transactions.

Signing Smart Contracts

Before smart contracts can be signed, they must satisfy an initial interface defined in the XCHNG API. This interface creates a generic set of requirements that all smart contracts must follow. All owners of a smart contract must verify and agree on the implementation of the smart contract before it can be deployed to the XCHNG network. Upon agreement, Owners sign the smart contract with their respective cryptographic keys. Signing the smart contract provides ownership and verification. Only Owners that have signed the smart contract can perform deploy, initialization and upgrade commands.

Deploying Smart Contracts

After a smart contract has been signed, it can be deployed to the XCHNG network that will execute the smart contract. Smart contracts are deployed via the XCHNG API by one of the Owners. Upon successfully deploying a smart contract, an address is created. This address is used to send additional commands and transaction requests to the smart contract. Once the smart contract has been deployed, it can be initialized by one of the Owners. Only an Owner of the signed smart contract can invoke a deploy command.

Initializing Smart Contracts

Once a smart contract has been deployed to the XCHNG network, an Owner can invoke an initialization command to the smart contract's address generated by the deployment. After successfully being initialized, the smart contract can begin receiving transaction requests. Only Owners of the smart contract can invoke the initialization command.

Upgrading Smart Contracts

The Owner(s) of the smart contract can invoke an upgrade command at any time. In order to upgrade an existing smart contract, owners must resign and deploy the new smart contract. After the smart contract has been deployed to the XCHNG network, Owners can invoke the upgrade command by supplying the existing smart contract's address. This will point the new smart contract to the original address so transactions can begin to process in the new version. It is up to the end user to manage the state of the smart contract when upgrading. Only an Owner of the smart contract can invoke the upgrade command.

Understanding the XCHNG Architecture

While the framework will be open, certain ecosystem partners, including Kochava Inc., intend to release tools to fast-track adoption of the XCHNG system across Sellers and Buyers. The XCHNG architecture is further described below and is made up of the Market, the Market Protocols, the Market Lifecycle, and the XCHNG Market.

Market

A market is a set of protocols that expedite the exchange of goods or services. Market protocols enable Buyers and Sellers to conduct transactions directly. Other network participants or actors can verify, rate, audit or otherwise operate in support of the transactions between a Buyer and Seller. The market protocols are decentralized. No single entity operates or governs the market. Transactions are transparent between designated participants in a transaction. Select transparency is available during the negotiation phase of a transaction based on the dynamics of the market protocols.

The market consists of the following: **inventory offers, buy offers, offer matching and settlement.**

1. Inventory Offers
   Inventory offers are statements of a seller's inventory. A Seller submits an inventory offer to the market via a Put protocol.
2. Buy Offers
   Buy offers are statements of a buyer's demand. A Buyer submits a buy offer to the market via a Put protocol.
3. Offer matching

A Buyer and a Seller submit their offers to the market. Each offer is added to the market list of offers. When two offers match, (i.e., the terms of both inventory offer and buy offer align) both Buyer and Seller jointly form an order. An order is a promise from the Buyer and the Seller for an exchange and is added to the market's order book via a Put protocol. Clients send transactions of an order to the market's ledger.

4. Settlement
   Clients (Buyer or Seller) interact with orders through Put and Get request. The XCHNG network validates that an order has been executed correctly. A cryptographic proof is generated by the Seller and verified by other network participants (i.e., Buyer, or auditor). Once the proofs have been verified, the network processes the payments and clears the order from the market's order book.

Market Protocols

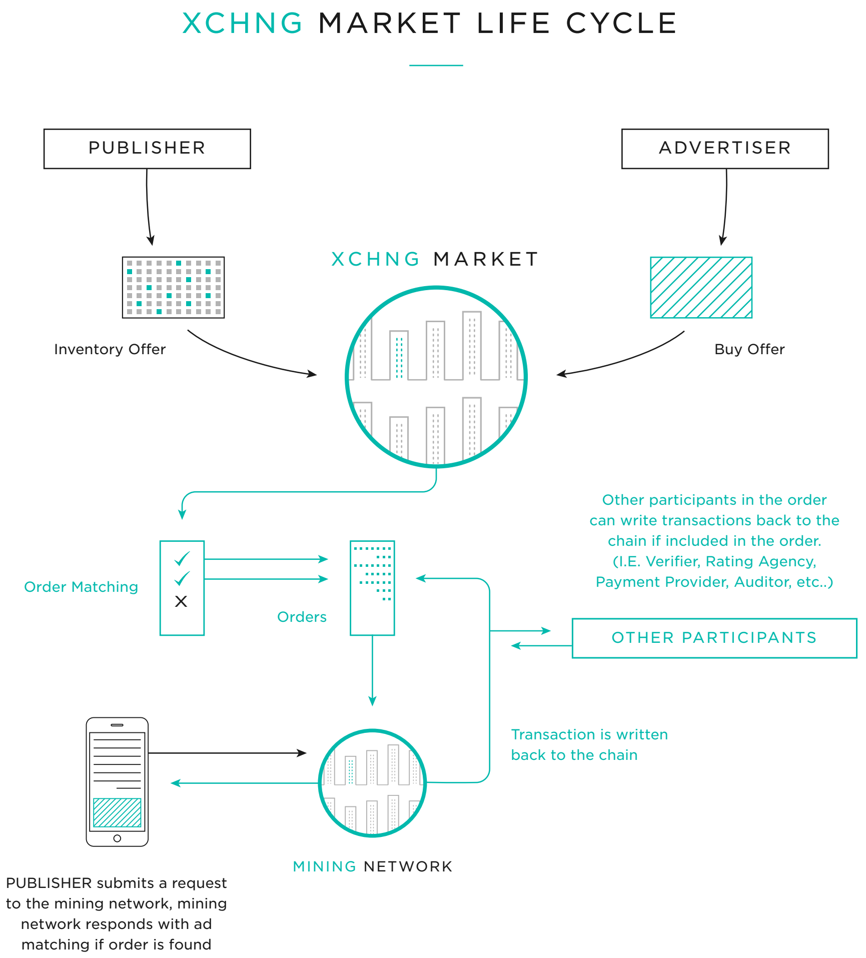
This section will provide a high level overview of the market's protocols.

1. Put
   Clients (Buyers and Sellers) can submit their offers via Put protocols. The various Put protocols are:
   - **Put.InventoryOffer:** A Seller submits an inventory offer through Put.InventoryOffer. The inventory offer defines what the Seller wishes to sell and may include pricing, description, quantity, etc.
   - **Put.BuyOffer:** A Buyer submits a buy offer through Put.BuyOffer. The Buyer's offer defines what the Buyer wishes to buy and may include pricing, search criteria, etc.
2. Get
   Clients (Buyers and Sellers) can access their offers via Get protocols. The various Get Protocols are:
   - **Get.InventoryOffers:** A Seller accesses inventory offers through Get.InventoryOffers. The response is a list of offers submitted by a Seller to the market. Each offer may include order details if matched.
   - **Get.BuyOffers:** A Buyer accesses buy offers through Get.BuyOffers. The response is a list of offers submitted by a Buyer to the market. Each offer may include order details if matched.
   - **Get.Order:** A Buyer or Seller accesses orders through Get.Order. Orders may be public or private depending on what the Buyer or Seller desires. If an order is private, only participants included in the order can view transactions pertaining to the order. Otherwise, the order is public and is considered open to the network.
3. Matching Offers
   After clients submit their offers to the market's offer list, the market can match offers programmatically or directly (i.e., by the Buyer and Seller)
   - **Put.MatchOffers:** Offers that have been introduced by clients are matched through the Put.MatchOffers protocol. Clients have the ability to match their offers directly. Additionally, the market can also programmatically match inventory offers to buy other offers. Matched offers form an order.

- **Put.SubmitOrder:** An order that has been created via Put.MatchOffers is submitted to the markets order book through Put.SubmitOrder. Once an order has been submitted, network participants can work to complete the order.

Market Lifecycle

The market lifecycle summary is depicted below.


XCHNG MARKET LIFE CYCLE
PUBLISHER
ADVERTISER
XCHNG MARKET
Inventory Offer
Buy Offer
Other participants in the order can write transactions back to the chain if included in the order. (I.E. Verifier, Rating Agency, Payment Provider, Auditor, etc..)
Order Matching
Orders
OTHER PARTICIPANTS
Transaction is written back to the chain
MINING NETWORK
PUBLISHER submits a request to the mining network, mining network responds with ad matching if order is found

1. Seller Client (publisher)

   At any epoch time (Unix epoch or Unix timestamp: the number of seconds that have elapsed since January 1, 1970, midnight UTC) may:

   - Submit new inventory offers via Put.InventoryOffer
   - Find matching offers via Put.MatchOffers
   - Submit matched offers to block chain via Put.SubmitOrder

2. Buyer Client (advertiser)

   At any epoch time may:

- Submit new buy offers via Put.BuyOffer
- Find matching offers via Put.MatchOffers
- Submit matched offers to block chain via Put.SubmitOrder

3. Matching Offers
    - Clients submit their offer through respective Put protocols
    - Offers are matched via Put.MatchOffers
    - Offer owners jointly form an order
    - Orders are submitted to the market's order book via Put.SubmitOrder
4. Settlement
    As client fills the order:
    - Both parties verify that the good/service was delivered
    - Seller generates proofs, other participants validate proofs
    - Buyer acknowledges valid and delivered transactions by sending payments to the Seller

XCHNG Market
The XCHNG market is a market implementation that facilitates digital ad buys, inventory selling, tracking, rating, payment, and audits. The XCHNG market implements the market protocols listed above.

XCHNG Clients
Publishers use a publisher client to introduce inventory offers to the market. Advertisers use an advertiser client to introduce buy offers to the market. Offers are matched through the XCHNG market's Put.MatchOffers protocol. During the matching phase, a negotiation phase occurs between the Seller (publisher) and the Buyer (advertiser).

During this negotiation phase, common time-based auction protocols are performed that allow for incremental movements from both parties. For example, Buyers and Sellers can input pricing thresholds that will automatically increase according to their respective offers during the negotiation phase of offer matching.

Zero-Knowledge Proofs
A common byproduct of a cryptographic proof is the gain of some knowledge in addition to now being convinced a statement is true. A zero knowledge proof attempts to avoid the share of knowledge between two parties. The two parties consist of a prover and a verifier. Furthermore, zero-knowledge proofs can be described as an interactive probabilistic proof that must satisfy three properties: Completeness, Soundness, and Zero-Knowledge.[16]

A zero-knowledge proof is said to be complete if the statement is true and the honest verifier (verifier that is following the protocol) is convinced of this fact by an honest prover. The proof is sound if one can never derive false statements using it. The proof is zero-knowledge if the statement is true and no malicious verifier learns anything other than the fact that the statement is true.

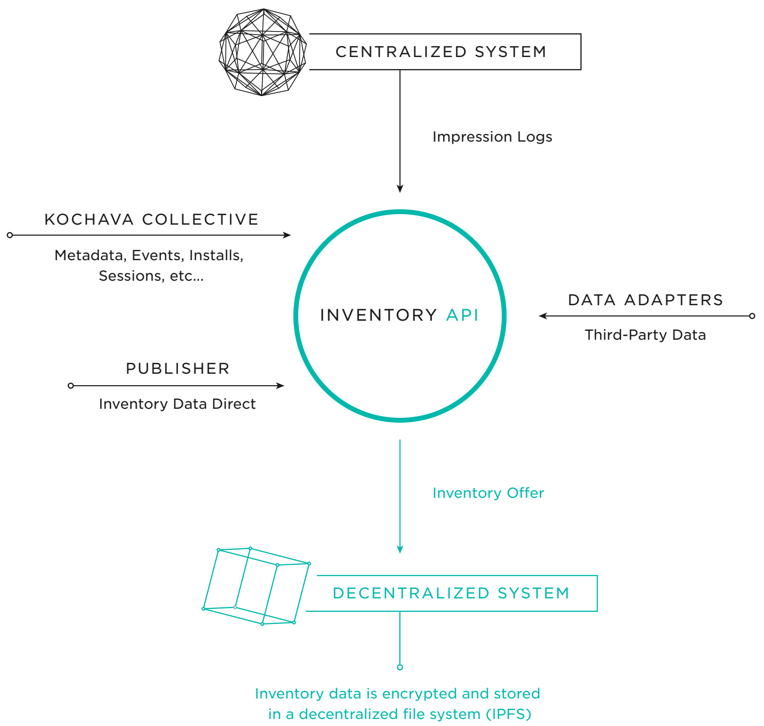
[16] http://www.cs.princeton.edu/courses/archive/spr10/cos433/lec17new.pdf

Insertion Orders

Once inventory is matched between publishers and advertisers, an order is submitted. In the XCHNG market, these orders may include terms such as pricing, frequency, partitioning, ad creative, duration, etc. A matched order becomes ratified into an insertion order by the participating parties. These smart contract IOs are made available to participants and the transactions that fulfill the order terms are written back to the IO transaction log.

A publisher will make a request to the network when an impression is available on the publisher's inventory. XCHNG ad serving miners answer this request by finding the appropriate IO for the impressions.

INTRODUCING INVENTORY
TO THE XCHNG SYSTEM



Introducing Inventory to the XCHNG System

Introducing inventory to the XCHNG system creates addressability links on the chain. This identifies that a particular device is addressable via the contributing media source that published the device inventory to the chain. It may also optionally introduce identity attestation (digitally signed attestations prove the authenticity of identity) for devices that can be targeted on the chain. The convergence of attributes about a device from multiple inventory sources verifies accurate existence of the device and the accuracy of the attributes of the device (e.g., device info, apps running on device, usage behaviors, location, or other metadata). This approach ensures that fraudulent inventory is not introduced onto the chain without negative consequence.

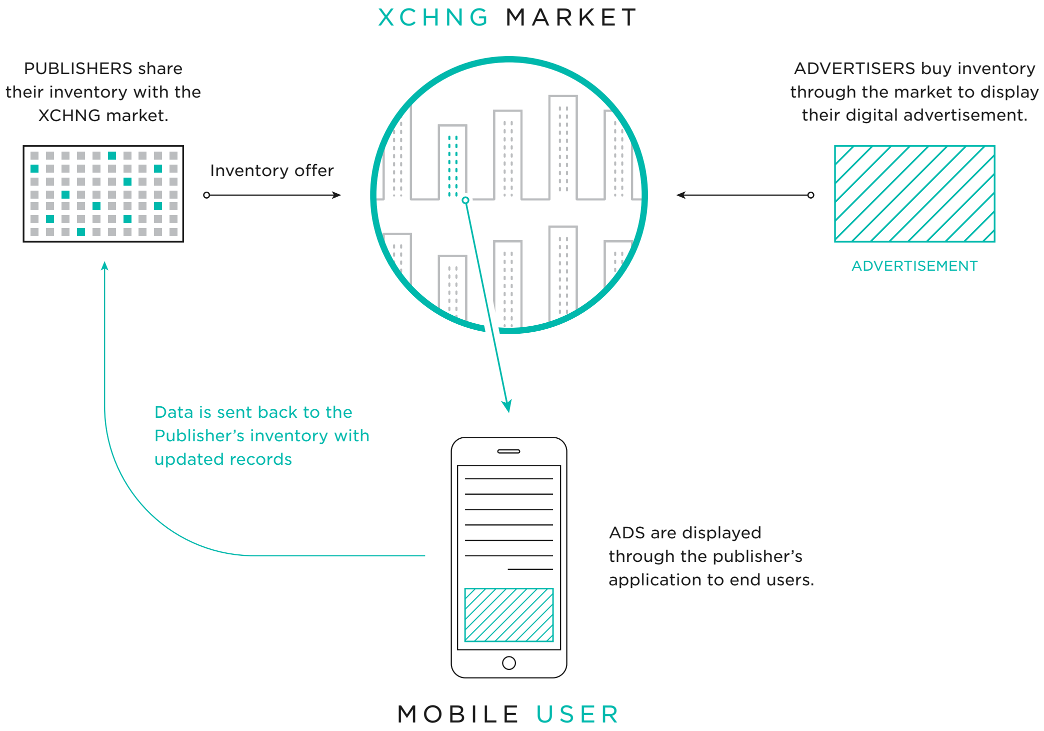
Incentive Model for XCHNG

To incentivize the participation of the community of inventory sources to publish their inventory of audiences and available volumes of impressions, XCHNG is designed to incorporate an incentive model to benefit supply sources.

Activating Inventory

Based on the inventory introduced onto the chain and smart contract IOs which commit delivery, inventory on the XCHNG system is activated by enabling ad impressions against tools provided by XCHNG with its open ad server and mediation server. By integrating these open tools for publishers, XCHNG enables easy adoption while also leveraging existing dynamics in advertising. Third-party ad servers and mediation servers will be able to include code from the reference implementation to run on XCHNG.

ACTIVATING INVENTORY


XCHNG MARKET
PUBLISHERS share their inventory with the XCHNG market.
Inventory offer
ADVERTISERS buy inventory through the market to display their digital advertisement.
ADVERTISEMENT
Data is sent back to the Publisher's inventory with updated records
ADS are displayed through the publisher's application to end users.
MOBILE USER

Additional Research

Network Sharding

Existing blockchain consensus models today (PoW, PoS, and BFT) often fall on different sides of a scalability spectrum. While PoW scales well with a large number of nodes, it suffers from high block latency. Alternatively, Byzantine fault tolerance models offer high transaction throughput but degrade with the number of nodes. As more peer nodes join, network bandwidth begins to limit transaction throughput. Typically, each peer in a public permissionless blockchain is required to process every transaction. The main principle around network sharding is to divide the network into smaller group of peers. This reduces the number of transaction each group is responsible for.

Side Chains

While encouraging research demonstrates how network sharding can increase transaction throughputs, XCHNG also incorporates side chains. Side chains refer to a parent/child relationship between two or more blockchains. Smart contracts that exist in a parent or root blockchain hold references to child side chains. This allows for subset peers to process transactions relating to a respective side chain, reducing the total number of transactions that they are responsible for. Each side chain is linked back to its parent chain using cryptographic proofs. The notion of daily rolling chains or DRC helps reduce the overall disk space required by peers responsible for maintaining a side chain. DRC summarizes transactions stored within a side chain into a cryptographic proof and writes it back to the side chains' parent chain. The XCHNG side chain model shares ideas from concept of Pegged Side chains.[17]

Relevance to Recent Token Projects in Digital Advertising

While the XCHNG project is compelling and incorporates the full circle of supporting digital advertising using blockchain technology, there are other projects in the blockchain domain that have been articulating their value in and around advertising. We want to highlight where we believe they fit and how our approach is different.

In particular, XCHNG sets itself apart from other projects because the system:

- Enables all actors in digital advertising to participate in ways that they currently participate (avoiding the revolution deployment and encouraging the evolution deployment instead)
- Creates new ways for incumbent actors to operate at scale
- Creates new ways for incoming actors to operate at scale—driving more competition
- Provides a clearly articulated path for advertisers to buy at scale with commercial tools running on top of a blockchain implementation (e.g., Kochava)
- Provides a clearly articulated path for publishers to leverage existing monetization strategies and slowly convert to XCHNG as monetization using XCHNG is demonstrated

[17] https://blockstream.com/sidechains.pdf

adChain

While adChain mentions a future that could support and assist with attribution or end-to-end transactional support via blockchain in advertising, the primary purpose of adChain per their white paper is to address fraud reporting by advertisers to publishers. adChain and XCHNG are not mutually exclusive; the adChain initiatives could play a role with XCHNG in the future.

AdLedger

AdLedger is not backed by a specific token but is instead a consortium of like-minded executives focused on standardizing around blockchain technology. Kochava is interested in working with AdLedger and would propose that the XCHNG system be the real-world manifestation supporting the consortium objectives.

Basic Attention Token (BAT)

The Basic Attention Token is primarily focused on creating a relationship between end users and publishers to both protect the identity of consumers and enable them to participate in the value chain of advertising. BAT and XCHNG are not mutually exclusive; the BAT initiative could play a role with XCHNG in the future.

Conclusion

In summary, the digital advertising ecosystem is ripe for a revolution. Blockchain is the disrupting technology that promises solutions to some of the greatest challenges facing the industry today: inefficiency, fraud, lack of transparency, and lack of standardization. In its peer-to-peer, decentralized nature, blockchain offers a new paradigm that evens the playing field and benefits all participants. Kochava is uniquely positioned to bring the blockchain solution to the digital advertising ecosystem.

OnXCHNG PARTNERS

The success of XCHNG will be directly related to adoption by the digital advertising ecosystem, which, in turn, will be dependent on the framework meeting the requirements of its participants and truly providing a more secure, transparent and efficient system. Kochava Labs has sought key partners to join the project. Each will add expertise and guidance as well as added exposure. Kochava Inc. is an initial Measurement Provider, and the following OnXCHNG Partners for all categories joined at the end of 2017: AerServ, AppLift, Appodeal, Chartboost, Datawallet, DataStream, DCMN, Feedmob, InMobi, Instal, Kiip, Parrable, Payability, PubNative, Snap Interactive, Sulvo and YouAppi. Information on each of these partners will be included in an updated white paper draft in 2018.

Kochava Inc. is ideally positioned to be the first referenced Measurement Provider on XCHNG.

About Kochava Inc.
Kochava Inc. (www.kochava.com) offers a unique, holistic and unbiased analytics platform to plan, target, measure, and optimize media spend. Its platform for mobile and connected devices combines potent features and global coverage with thousands of network and publisher integrations, allowing advertisers to target audiences and measure campaign performance with precision. Real-time customizable visualizations give users fluid access to a full spectrum of data points, providing robust segmentation capabilities and real-time actionability. Yielding the most powerful tools in the ecosystem, Kochava Inc. is chosen by brands across industry verticals to measure the largest and most sophisticated ad campaigns.

Kochava Inc. is Uniquely Positioned to be a Trusted Measurement Provider on the XCHNG Framework
Kochava Inc. is integrated with nearly all mobile media sources in existence including Facebook, Google, Snap, Twitter, and Oath as well as leading independent vendors such as AdColony, AppLovin, Vungle and InMobi. In all, there are over 3,000 ad networks and media sources that are technologically integrated with the Kochava Platform. In addition, the Kochava Media Guide has over 50,000 registered publishers covering display ad inventory. Today, Kochava Inc. is the system of record that provides attribution based on advertiser configuration for their ad campaigns, representing over $6B in ad spend measured each year.

Note the LUMAscape diagram of companies in the digital advertising ecosystem on page 9 of this white paper. Kochava Inc. already works with all sectors of the diagram. The scope and reach of these long-held industry relationships are significant.

Kochava Inc. presently behaves as a Measurement Provider without the associated architecture and framework accounted for via the XCHNG blockchain. Kochava Inc. is uniquely positioned to ‘bring along’ a very large and complex industry to start standardizing around the blockchain for advertising.

Kochava Labs SEZC, the research and development subsidiary of Kochava Inc., is the architect of XCHNG and Kochava Inc. stands to be a juggernaut first reference implementation. More than a project conceptualized by blockchain engineers with nothing more than a hope for industry adoption, Kochava Inc. and the other OnXCHNG Partners intend to leverage their authority and experience in the ecosystem to drive sweeping conversion to the XCHNG blockchain. Further, because Kochava Inc. is not a media provider, it is immune from the inherent conflict of interest that exists when a supply partner attempts to “grade their own homework.” Indeed, any blockchain initiative within advertising that stems from a publisher or their own ad inventory will be viewed skeptically through the lens of interest conflict. This is why independence from media and independence from venture capital demonstrates the motivations behind the XCHNG system.

XCHNG Team Members

Charles Manning
CEO, Kochava Inc.
Director, Kochava Labs SEZC

Charles Manning is the founder and CEO of Kochava Inc., the leading mobile attribution and analytics platform serving tier-one advertisers worldwide. For nearly 20 years Charles has been creating technologies that use data for system optimization, ranging from business service management (BSM) to information technology (IT) to attribution analytics, and most recently blockchain. Charles began his career at Oracle, and later held executive and C-Level positions at M-Code, Managed Objects, and PLAYXPERT.

Prior to founding Kochava, Charles founded PLAYXPERT–which started as a gaming technology platform. After licensing the PLAYXPERT technology to Razer, Charles built a team that focused its time on building engagement platforms for entrepreneurs and agencies. Upon realizing the need for a standard platform for effective attribution or post-install analytics in mobile–Charles and his team built one, and Kochava was born. The Kochava technology is now integrated with more than 3,500 networks and publishers and is trusted by hundreds of brands including the biggest names in mobile gaming, news and media, and consumer goods.

Breaux Walker
SVP Blockchain, XCHNG

Breaux Walker is an international blockchain and tokenization business development leader. As SVP Blockchain at Kochava, Breaux is responsible for business development of the Kochava-sponsored open source blockchain project, XCHNG. Previously, Breaux was the SVP, International for Union Mobile Fintech, a publicly-listed Chinese fintech company. Prior to joining UMF, he was a partner at Kuan Capital, where he invested in fintech, mobile, and Internet companies in China.

Breaux has 10+ years of investment banking experience and was a managing director with JMP Securities' investment banking group. He oversaw the China investment banking team and managed the company's joint venture with China Merchants Securities. Throughout his career, Breaux has been an entrepreneur and banker in the mobile and Internet sectors in the US and China, closing over $1B in transactions. He is fluent in written and spoken Mandarin Chinese.

Ethan Lewis

Blockchain Architect, XCHNG

Ethan is the primary architect of the XCHNG framework. He holds a master's degree in CS from Wright State University and previously held the position of Lead Build/Automation Engineer with IBM's B2B Cloud Services Division writing software and training new team members. Ethan has worked in VR and AR, and developed Sense and Avoid projects for unmanned aircraft systems as well as designed and developed proof-of-concept and integration test systems for internal applications, always with a focus on optimization for speed and efficacy. Skilled in Golang, Java, Python, C++, and many other languages and technologies, Ethan has a particular passion for and experience with blockchain and distributed ledger technologies.

David Matt

General Manager, Kochava Labs SEZC

David serves as inside counsel and runs the Cayman Islands office for Kochava Labs SEZC. He holds a JD from Gonzaga University School of Law. David's areas of expertise include corporate law, M&A, intellectual property and data privacy. Previously, David was a business consultant with DMS Worldwide for seven years. He also spent 14 years as an entreprenuer on various ventures primarily in apparel manufacturing.

Doug Lieuallen

Director, Kochava Labs SEZC

Doug Lieuallen has served as a financial executive for 25 years, with experience ranging from start-ups to public entities, across technology, advertising, and retail industries. As the CFO of Kochava, Doug plays a strategic role in the overall management of the organization. Primary responsibilities include accounting, FP&A, treasury, M&A, legal, and administrative functions.

Prior to his appointment to Kochava, Doug held multiple finance and accounting leadership roles, most recently as the Senior Director of Treasury Operations at the $700 million retailer, Coldwater Creek, and previously as the Finance Director for Wieden + Kennedy London. Throughout his career, Doug has been tasked with creating and funding scalable, global operations.

As a Director of Kochava Labs, he provides oversight and expertise for the Kochava-sponsored open source blockchain project, XCHNG.

Kimberly Manning
Brand Director, XCHNG
Kimberly has a long history of marketing experience specializing in brand creation and management. She is the brand director at Kochava Inc. and formerly was founder and principal of her own design firm for twelve years, providing branding, marketing, and content creation to tech, biotech, consumer product and non-profit clients. Kimberly has a particular passion around blockchain and how to make distributed ledger technologies accessible and understandable to a broader audience.

Matt Hrushka
Product Manager, XCHNG
Matt has been involved in the cryptocurrency space since 2015 and has a deep knowledge of distributed ledger technologies including blockchain. Additionally, Matt's professional experience in the digital advertising space makes him uniquely qualified to understand the application of blockchain to address the challenges of this particular industry. Matt previously served as the Mobile Marketing Manager at Rosetta Stone and, before that, was the Ad Operations Manager at Verve Mobile. Matt is the primary Contact for the OnXCHNG Partner Program and is passionate about bringing new partners into the XCHNG project.

A Deep Bench
Kochava Labs SEZC has contracted Kochava Inc. for development and marketing of XCHNG. In addition to the individual team members outlined above, the project has at its disposal the full bench of expertise represented by 150 employees at Kochava Inc., including management, development, marketing, and account services.

XCHNG Advisors

Kochava has been proud to welcome advisors to the XCHNG project who comprise a board of seasoned experts in all aspects of digital advertising, blockchain technologies, and cryptocurrencies. Their participation will continue to guide the development of XCHNG and the XCHNG Token.

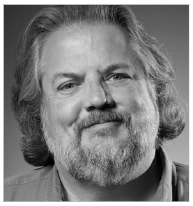
Mark Beck
VP Strategy at Murka

Paul Cheng
GM at Ericsson Emodo
Experienced Executive and Advisor with a demonstrated history in the internet, mobile, AdTech, MarTech and cryptocurrency/payment industries.

Terrence Coles
GM at AddApptr GmbH, Previously GM at Smaato

Mark Connon
Former Senior Vice President and Global Chief Mobile & Data Officer at AOL Platforms & Advertising

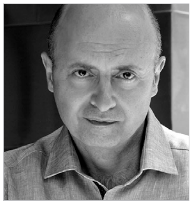
Jeff Coon
Former VP of Global Alliances at InMobi and previously Head of BD at Quantcast



Ernie Cormier
Formerly CEO of Nexage, Ernie specializes in P&L ownership, strategy, product, technology/engineering, marketing & brand, sales, business and corporate development

Paran Johar
Global CEO at Modern Marketing Summit

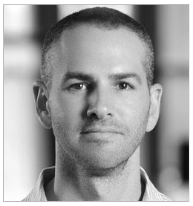
John Maffei
CEO at Matcherino
Former CEO Servicemesh, Former President ZAM Network



William Mougayar
Advisor, Investor, Mentor to Tech Entrepreneurs and Founders on Strategy, Marketing and Growth. International speaker and Author of *The Business Blockchain: Promise, Practice, and Application of the Next Internet Technology*

Stephane Panyasiri
GM of EMEA for Kochava Inc.
Former CEO at SEA Gaming Pte Ltd

Krish Sailam
VP of Programmatic Strategy, West Coast at Cadreon



Jeremy Sigel
Global SVP of Partnerships & Emerging Media at Essence

Andy Sippel
SVP of Advertiser Perceptions, previously SVP of USA Today Sports Media Group

David Wachsman
Founder and CEO at Wachsman, the world's largest blockchain public relations agency

Bob Walczak
Former EVP of Global Product at WPP's programmatic ad-buying platform, Xaxis

Kevin Weatherman
VP of BD at OneSignal and previously VP of BD/Sales at MoPub and Director of Global Publisher Sales at Twitter

David Weild, IV
Former Vice Chairman of NASDAQ
Founder, Chairman and CEO of Weild & Co. Inc., parent company of the investment banking firm Weild Capital, LLC. Weild is also known as the "father" of the JOBS Act, and has been involved in drafting legislation for the US Congress.