BitClave:

Decentralized Search Ecosystem

The $550B Ads Market is About to be Disrupted by Blockchain

Distributed Blockchain-Based Smart Contracts
for Connecting Consumers and Businesses

http://www.bitclave.com

Draft v 0.9.2

June 2017

Executive Summary

BITCLAVE ACTIVE SEARCH ECOSYSTEM IS A PLATFORM THAT ENABLES DIRECT CUSTOMER-TO-BUSINESS INTERACTIONS WITH NO NEED FOR INTERMEDIARIES.

When it comes to online advertising, businesses are forced to pay exorbitant amounts of money to “middlemen” in order to reach a captive audience for their promotions. However, the promotions often get placed among many other ads clogging up the space on crowded banners, or simply end up in someone’s spam box. Businesses also have little to no guarantee that the traffic they generate on their promotions is genuine. In fact, nearly 50% of all advertising traffic is generated by bots, essentially defeating the entire purpose of advertising. Sellers pay for “impressions, views, and clicks” resulting in extremely low conversion rates, having only loose correlation to return on investment.

Offline advertising is a similar story. More often than not, offline advertisers promote content with a “hit or miss” mass mailer mentality. Hoards of messages are slammed into users' faces with little or no targeting, resulting in a dubious correlation between offline ad dollars and return on investment. This, along with other factors, contributes to extremely low conversion rates. Promotions are largely delivered to those who simply do not care for the product or whose attention is likely focused on something else.

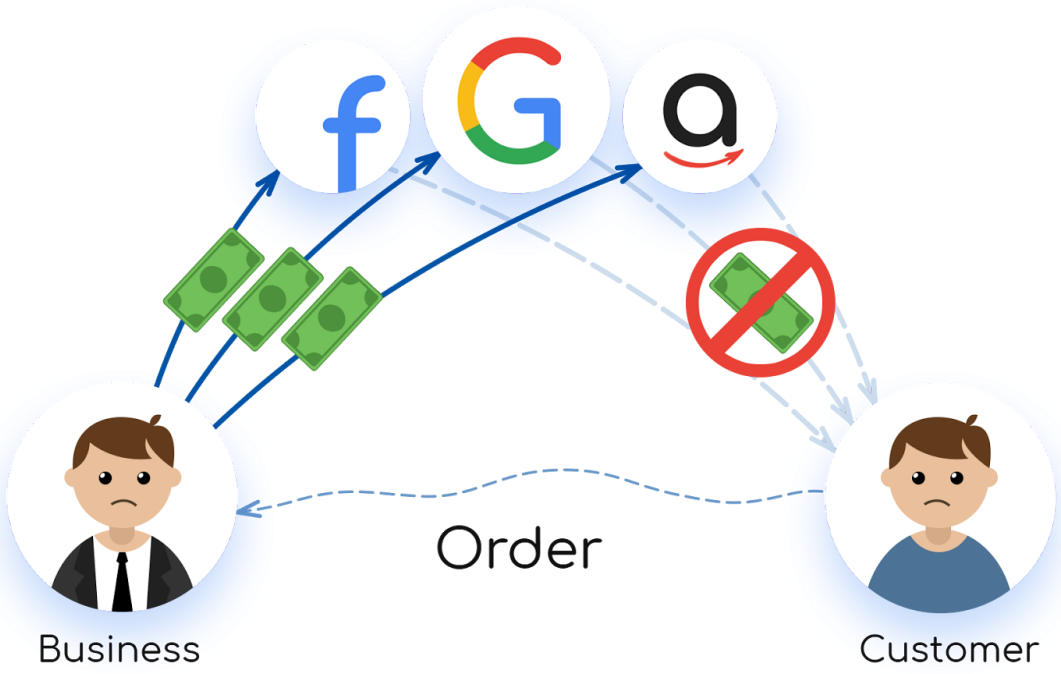
These ineffective measures, both offline and online, negatively impact the whole service value chain. The more companies are forced to pay to “middlemen”, such as Google and Facebook, the more money consumers have to pay for products and services. Businesses end up losing money, and consumers end up paying more for less value, creating a lose-lose situation.

In order to counteract the problems described above, BitClave proposes a system in which the intermediaries are eliminated and interactions are facilitated by the network itself. Instead of paying any “middlemen”, companies automatically make personalized offers directly to consumers who have opted in for the service.

In this ecosystem, consumers have control over their own data and can opt into advertising and analytics services by retailers through the use of smart contracts. This not only ensures that companies are making their offers to an audience that is more inclined to view and interact with their offerings, it also allows consumers to earn money for viewing these promotions.

This system also ensures increased user privacy. ”Free” services, such as Google and Facebook, often sell user data to brokers. With the *BitClave Active Search Ecosystem* in place, however, this is no longer a concern as companies sell their promotions to consumers firsthand.

Problem Description



TODAY'S FRAGMENTED SELLER-ADVERTISER-CONSUMER VALUE CHAIN MISSES THE MARKET OPPORTUNITY.

Advertising—a market worth nearly 550 billion dollars[1]—is broken. Businesses today contend with myriad middlemen across the advertising stack. The dominant advertising companies (*e.g.*, Google, Amazon, Facebook) charge exorbitant fees to reach users. Businesses receive no guarantee their ads will convert to sales, or even that their ad traffic is genuine—in fact, nearly 50 percent of all ad traffic is generated by bots, essentially defeating the purpose of advertising itself.[2,3] The more businesses pay for ads, the more money consumers have to pay for products. Businesses end up losing money and consumers end up paying more for less value, creating a lose-lose situation.

Large online advertising companies are also missing the enormous market opportunity because they are not motivated to optimize the seller-consumer value chain (*i.e.*, conversions). These companies instead work tirelessly to locally-maximize their own profits by increasing the cost of

[1] Statista, "Global Advertising Market - Statistics & Facts", Available https://www.statista.com/topics/990/global-advertising-market/, accessed June 15, 2017.
[2] Incapsula, "Bot Traffic Report 2016", Available https://www.incapsula.com/blog/bot-traffic-report-2016.html, January 2017.
[3] G. Sloane, "Nearly 25% of Video Ad Views Are Fraudulent, and 6 Other Alarming Stats", Available http://www.adweek.com/digital/7-things-you-need-know-about-bots-are-threatening-ad-industry-161849/, December 2014.

desirable ad placements and click-thru rates, while hoarding their troves of user-data behind walled-gardens of fragmented, proprietary ad-networks.

Today's centralized ad networks impede market growth because they aren't optimized for seller-to-consumer conversions.

GLOBAL MARKETS DEMAND SOLUTIONS THAT RESPECT CONSUMERS PRIVACY. BUT PERSONAL DATA IS VALUABLE, AND DOESN'T COME FOR FREE.

Large online ad companies are also facing regulatory pressure to protect consumer privacy. Recent changes to the ePrivacy Directive and the General Data Protection Regulation (GDPR) in the European Union (EU) highlight the emerging trend of Governments forcing technology companies to build-in consumer privacy by design.

It has long been realized that actionable consumer data has intrinsic value—encoding this value into the data with blockchain provides a novel mechanism to securely transact data while maintaining consumer privacy (identity anonymization) and control.

Global-market privacy requirements are a key near-term driver for technology solutions enabling anonymized search over large consumer datasets.

A BRIEF HISTORY OF ADVERTISING: MARKETS THAT STIFLE INNOVATION ARE ALWAYS SUSCEPTIBLE TO TECHNOLOGY-BASED DISRUPTION.

Advertising has emerged as a crucial component of business operations since time immemorial. The global spread of the printing press, one of the key inventions of modern society that enshrined content publishing as a new branch of media, is incomplete without an account of the role of content marketing.

The history and evolution of advertising has tracked, and in many cases been the impetus and driver for, progress in communications technology. The yellow pages, a collection of print directories for businesses that played an important role in extending telephony to enterprise, was funded by selling advertising space.

The rise of the Internet accelerated the reach of advertising but also changed the ways in which people respond to ads. Yahoo, once the de facto ingress point for the Internet, was in many ways the digital analog of the yellow pages and the bridge to today's Internet landing pages.

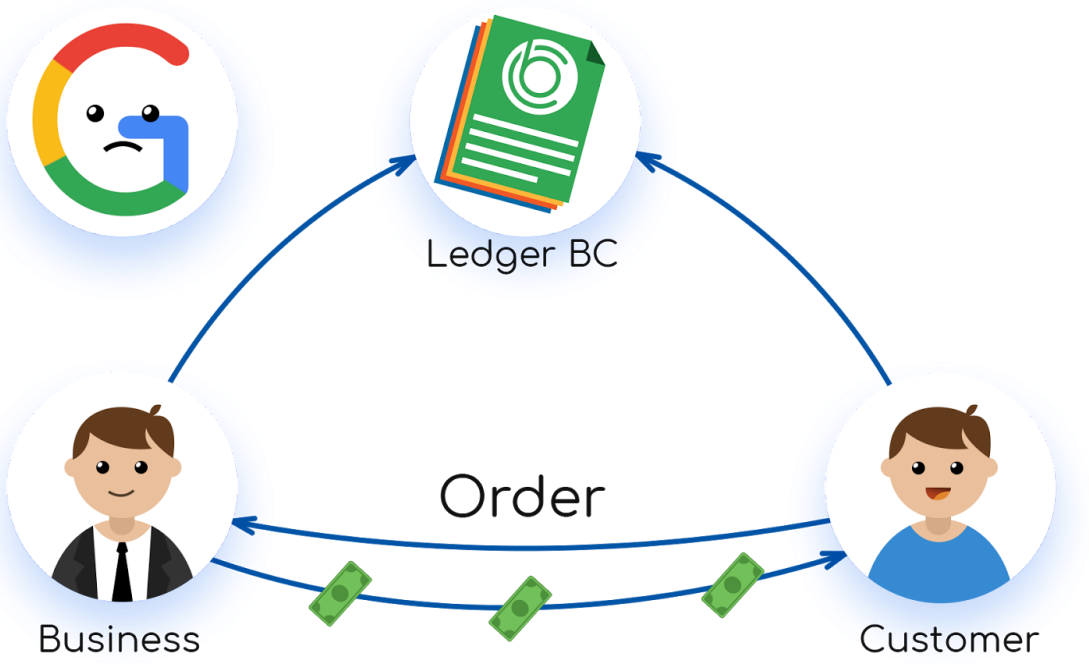
The media for advertising have become more efficient with time but the core function of advertising, creating relevant connections between people and services, has seen only marginal improvement. Search and social media—although distinct in their customer facing services and revolutionary in their crystallization of large-scale high-performance knowledge and social graphs—follow a very similar business model dating back to before Yahoo and the yellow

pages. We argue that the advertising model of the "middleman" is not only superfluous but a backstop to business value.

The next step in the evolution of advertising is truly revolutionary. Blockchain is a powerful emerging technology that enables mutually distrusting parties to engage in mutually beneficial co-enterprise without the requirement of a central authority. Decentralized search is the next step in this progression of advertising as a medium for people and business to connect. BitClave applies these powerful design patterns to reimagining a more transparent and meaningful medium for people and businesses to engage in value creation.

The advertising industry is once again ripe for technology-enabled disruption—BitClave technology enables 1) scalable, secure, anonymous search over huge datasets; 2) data privacy; and 3) a mechanism to transact valuable data, with attestation.

Solution Overview



BITCLAVE'S DECENTRALIZED SEARCH ECOSYSTEM REALIZES UNPARALLELED MARKET EFFICIENCY ACROSS THE CUSTOMER-TO-BUSINESS VALUE CHAIN.

BitClave's *decentralized* solution enables companies big and small to participate in a common ecosystem. The innovative *search* technology enables sellers to pay directly for outcomes, optimizing marketing spend for results; users and other data providers are paid on the data's value, measured by conversions (not clicks); and consumers gain access to monetary incentives and lower-cost goods while gaining control over their personal information. BitClave's *ecosystem* uses the blockchain to encode the value of data in the data itself, enabling

transactions that are both anonymous for consumers (until such time as they chose otherwise, *e.g.*, complete a purchase transaction), while providing attestation required to charge sellers for outcomes and pay users for their data. Consumer privacy is built into the very fabric of the BitClave decentralized search ecosystem by design.

BitClave makes it possible—for the first time—to optimize the seller-consumer value chain. In the BitClave ecosystem, third parties are incented to provide data that maximizes seller-consumer market efficiency—data, ads, and offers that result in lowest-cost outcomes. Analytics providers may participate in a rich app ecosystem, and are rewarded for innovation, paid with the proceeds of increased overall market efficiency. By eliminating the waste from today's large advertising network solutions, everyone wins. BitClave's open ecosystem ensures innovation will continue in the advertising market as technology continues to evolve.

Use Case Study

The potential for disruptive applications built on the solution proposed here are significant. Throughout this document we refer in brief to several use cases with offline and online promotions and purchase components. Some example use cases are presented here followed by an illustrative use case study of the automotive sales retail space, with mixed online and offline components, to highlight the architecture and benefits to the ecosystem participants.

In the rentals and retail space, properties may be managed and traded using the combination of Internet of Things attestation points and an underlying seamless rewards element of distributed retail ecosystem. An off-the-shelf home security system interfaced with a retail blockchain and enforced by smart contracts would enable property owners to remotely manage and rent their property securely with, from their perspective, what would amount to anonymized paying tenants (a decentralized AirBnB app). A prospective renter would simply open this service to see which units are available nearby, gain authorized access with or without a host, and decide how long to stay whether a few minutes or a few months. Or a real estate agent could invite prospective buyers for a home showing using a smart contract backed promotions program and follow up with additional offers based optimized for each buyer's market for the home. In the retails shopping and local business space, Many brick-and-mortar retail businesses have seen significant disruption from online retailers. An activity-based reward platform with strong support for authorized data sharing and collaborative market-making for co-located business could signal the return to shopping centers and complement online retailers with plug-and-play support for real world presence. The professional services industry benefit significantly from the foundational attributes of a public blockchain and the direct professional-to-client interactions supported within BASE.

AUTOMOTIVE SALES

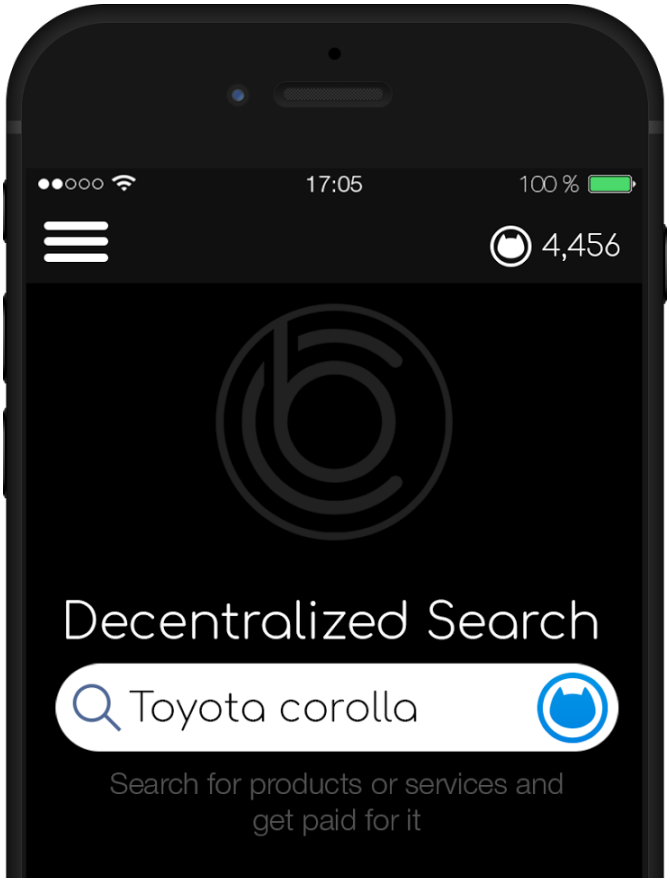
The first use case we describe is within the automotive industry. As in many sectors, customer acquisition is a business critical and costly sales component. In the car dealership industry, this

factor is key to operating a successful distribution network. Automotive dealers typically spend up to $200 per qualified lead by promotion on general-purpose online referral sources (like Google AdSense or Facebook's Audience Network) and dealership-facing products for popular customer-facing car information and pricing services like TrueCar—with the automotive-focused gateways for leads being both more costly and more efficacious than the general-purpose gateways.

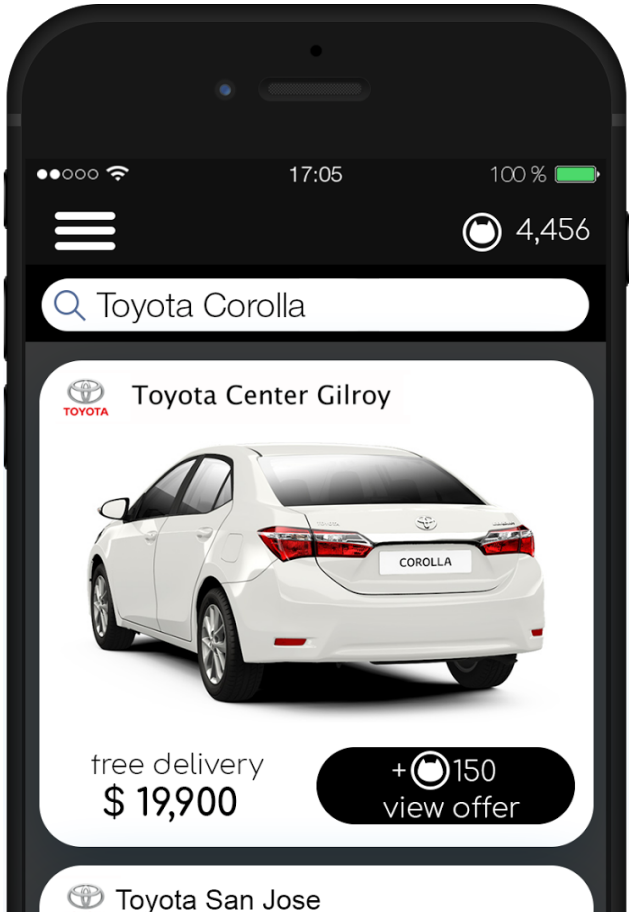
They compete via keyword on a national, regional and local basis against other dealers; as well as against other automotive-related services such as leasing, insurance and financing. This digital advertising is combined with traditional marketing that includes local broadcast, radio, billboards and sponsorships. It is also supported by the conventional regional dealers association, where local dealers pool marketing dollars to enable greater ad buying efficiency in a particular area as well as pool data resources such as customer purchase history. All this adds up to an expensive, complicated, competitive environment. An environment that moves consistently in favor of supply, not demand. So even as the overall margins on new vehicle sales has declined, the cost of customer acquisition has tightened, impairing the dealers ability to operate successfully. This cost pressure is only heightened by the rapid depreciation rate of car lot vehicles.

In practice, several hundred dollars is often the threshold between a lost lead or a happy customer leaving the lot in a new car. Today, car dealers provide benefits such as $100 prepaid gas cards or 6-months complimentary roadside assistance to help close deals. Additionally, these "deal sweeteners" are provided to car dealerships themselves by the automotive-focused referral services as incentive to justify their high membership costs. In terms of sales and satisfied customers, the budget spent on acquiring lead referrals is better spent on direct promotion offers to the customer. A network that facilitates direct customer-to-business engagement and where qualified leads are the concomitant of those engagements is precisely the solution for redirecting wasteful targeting expenses to enhanced customer relations efforts.

In the BitClave Ecosystem, an automotive dealership will have the opportunity to display their promotions and advertisements directly to a potential buyer; utilizing the precise targeting that the BitClave Ecosystem provides. At the same time, the dealership will be guaranteed that their content is viewed by legitimate buyers and not pseudo-viewers, who are either not interested in the content or simply fake. The dealership will have the option to filter out those whom the content is shown to; selecting criteria such as the consumer owning a car for more than two years or having a child who recently became eligible to drive.



The history and profile of the consumer will be stored securely in the ledger, ensuring that the dealership's money is not going to waste. Each consumer will have an associated "rating" in the system, calculated by analyzing the frequency of the advertisements the consumer receives and their conversion rate on these promotions. With access to those ratings, the businesses can assess the value of the consumer target given their past behavior. For instance, if the consumer indexes high on promotional messages received, but low on action taken against those promotions, the business may conclude the likelihood of future purchase is low and decline to target. Similarly, analysis of a given customer's activity over time enables businesses to identify customers who have shown demonstrated interest in a product or service provided by competitors but have not completed a purchase; leading to insights regarding how to improve services and promotions in a cost-effective manner. This ensures to businesses that their advertising budget is likely to lead to increased return on investment, an assurance that simply does not exist with the current advertising model. Thus, by eliminating any potential intermediaries and utilizing the BitClave Ecosystem, the business is able to utilize the system's precise targeting, at a fraction of the cost, to locate consumers that are amenable to promotion and more likely to complete a product purchase, while the pool of interested buyers are rewarded with incentives of up to $50, for example, for viewing and interacting with the promotion.



Technology Overview

BITCLAVE IS A STARTUP COMPANY BASED IN MOUNTAIN VIEW, CALIFORNIA, PROVIDING SEAMLESS CUSTOMER REWARDS AND PAYMENTS SOLUTIONS.

One of the primary innovations that BitClave is focusing on is a distributed blockchain-based system, called the **BitClave Active Search Ecosystem (BASE)**, which allows the storing and managing of vast amounts of data consisting of records of customer *activities* from an unlimited and variegated number of *attestation points*. Some examples of customer activities include entering a particular building, accessing a particular Wi-Fi network, making a purchase, opening a mobile app, and requesting a delivery online. These activities include any event that is shared with and can be automatically processed by enabled attestation points such as cameras, web sites, mobile devices, apps, cloud servers, WiFi routers, and Bluetooth hubs. Instead of releasing and selling this data to monolithic advertising service providers, the attestation data is contributed by users in a decentralized manner using blockchain, similar to the way Bitcoin is implemented except here the emphasis is on retails activity as opposed to currency. Further, the

data bundles associated with each attestation record remain under the management domain of the contributors.

Each block posted into the blockchain contains anonymized information about a particular activity. The block anonymization is done in a way that allows only specific groups of authorized parties to attribute multiple blocks to the same customer. For all other parties, the data is be untraceable to specific individuals but still valuable for statistical and data aggregation purposes. This gives the customer control over what data is allowed to be created, shared, and accessed, all through the use of blockchain and smart contracts.

Ethereal Consumer Activity Token

On top of this distributed activity data collection system, BitClave is introducing a token, called the BitClave **Consumer Activity Token (CAT)**, to be used internally within the blockchain among the participating parties. CAT tokens will be used to facilitate rewards within the system for all sorts of services that available on the BASE. The CAT-based market puts power into the hands of producers and consumers, instead of focusing power on large advertising companies that collect and profit from customer data surreptitiously. Customers and retailers can interact directly through transparent and consumer-authorized message posts and data bundles on the public blockchain, and additional parties can contribute as service providers by creating analytics capabilities that operate over the data in the blockchain.

The initial vision for the CAT token is based on Ethereum technology, an open source, blockchain-based distributed computing platform with smart contracts. These cryptographically secure smart contracts are stateful applications stored in the Ethereum blockchain, fully capable of enforcing performance. The token is derived from customer activity. While Ethereum is the initial target, we may transition to a different blockchain technology if appropriate.

In contrast to centralized and hidden ad models, consumers benefit both from more personalized and relevant services as well as from the value generated by their contributed data. Additionally, businesses benefit from more direct access to interested customers and a more measurable correlation between promotional expenses, customer activity, and return on investment.

Retail Vision and Value Statement

Commonly, online advertising has been employed by businesses to reach potential customers. With online advertising, service providers and businesses spend significant portions of their marketing and advertising budgets on impressions, page views, and click throughs. This approach only loosely translates to increased sales for businesses and increased value for customers, in large part, because the medium used to connect customers with businesses (i.e., the combination of popular “free” web services and the murky web of hidden ad networks) actually inserts a wide and costly gulf between the two. We believe that a blockchain-based

system is well suited for enabling customers and businesses to *directly* connect in mutually beneficial market activity throughout the entire promotion to purchase value chain.

With decentralized search, previously wasted ad dollars are redirected to promotion and rewards programs that reach only genuinely interested customers by increased incentives to new customers and increased benefits to loyal customers. With a well-devised blockchain, customer profiles can be elevated from shadowy privacy-invasive metadata, owned and controlled by third parties, into authorized attestations traded in a transparent activity-driven marketplace where customers and brands alike share in value creation. With a new form of rewards founded on activity, value creation is captured on a public blockchain without disclosing personally identifiable information (i.e., providing unlinkability and anonymity).

This vision is achieved by supporting distributed collection and verification of customer activities in both the online and offline retail worlds, as well as profiles and preferences that can be specified directly by the customer, to create a token-based ecosystem for demand-driven marketing and retail with a low barrier to entry for all parties.

Overall, the system we are developing has two major components:

- The **anonymized activity ledger** (or simply, activity ledger or ledger) is a decentralized account of relevant customer and retailer activities, including any retail activities that are observable by some party in the ecosystem (e.g., visiting a retail store, buying a product, rating a retailer). Personally identifying information is masked using an *activity ledger anonymity* mechanism to selectively hide individual customer/retailer identities while still allowing certain types of decentralized analytics to be computed over the ledger data, and other ledger entry fields may contain encrypted data that is only available to specific groups (e.g., conditioned release in response to achieving a smart contract trigger). Based on the ledger entries, group members will be able to perform *activity ledger analytics* operations to identify activity features or retail trends that enable marketing or business opportunities, for example offering discounts for a popular item or inviting customers to attend a product demo.
- On top of the activity ledger, we are employing a **token exchange** to provide incentives and rewards across interested parties and groups. Entities can earn tokens by contributing activity data to the ledger or through creation and execution of smart contracts with other parties.

The activity ledger and token exchange components are discussed in more detail in the following sections.

Anonymized Activity Ledger

The anonymized activity ledger is the foundation of the retail ecosystem, providing a decentralized capability for the crowdsourcing and sharing of data describing customer and retailer activity. The activity ledger facilitates a wide variety of analytics capabilities that leverage

the activity data from customers, stores, mobile apps, and websites across different retail domains. As mentioned previously, any party who can attest to activities in a retail domain — whether the retailer, the customer, or a third party — can contribute anonymized activity data to the ledger, and any party who can access the ledger entries can potentially get value from the data, in accordance with the terms specified by a loyalty program or other contract-based agreement between retailers and customers.

Activities as Blockchain Entries

For clarity, we refer to any entity capable of observing retail activity and establishing a notion of customer and/or retailer identity as an **Attestation Point (AP)**, noting that an AP may exist in either the digital or physical domain. Examples of APs include smartphones, mobile apps, wireless network elements (such as Wi-Fi access points and Bluetooth beacons), point of sale terminals, landing pages on retail websites, HTTP redirects, and so on. Note that many of the AP examples correspond to systems that are already deployed in many online and offline retail stores and currently serve other purposes for the retailer or customer. Any AP is capable of creating data entries to the ledger, but only those APs owned by the customer or by an entity with an existing relationship with the customer (e.g., via service registration, loyalty program, or smart contract) will be able to include encrypted information about the customer's identity.

Users contribute their data in several ways. They update profiles with their personal data and are tied to biometrics or multi-factor authentication for account protection. They can configure what information to give to the registry. For example, users can enable or disable geolocation or specify additional condition and constraint rules.

The second source of data is the history of the search for goods and services through applications built on the basis of the ecosystem. These data are anonymous and users can manage them themselves.

To record data on visiting other sites in the register, an authorization button is used, similar to the button for password authentication via Facebook. Web sites can embed an authorization button. At the same time, the reward for this data is received both by the user and the website using this button.

Retail AP devices and software will be able to post activities that include identifying information about the corresponding store, either using pre-programmed identifiers or something that can be learned through the observation itself. For example, consider an attestation point that incorporates an the infrared sensor used to open the entry doors when people arrive and a Wi-Fi network providing complimentary connectivity to staff and customers. The attestation point can be pre-programmed with the identifiers of the car dealership and the specific building, but it will not be able to identify individual customers. However, if the attestation point is integrated into the car dealership's customer loyalty database, then identification recognition software based on time of arrival and network trace can be employed to recognize customers who have

opted into the program and have contractually allowed the car dealership to include their anonymized identity information in the activity report. Customers who have *not* opted in cannot be identified by the AP, so the activity report does not include any customer identity in this case. Additionally, an AP may initiate new or short-lived business-to-customer relationships.

Independent of the identification of the customer, the car dealership's AP can identify specific activities including customer arrival, departure, and cars shown in the lot. Similarly, the point-of-sale terminal can record what the customer actually purchased, so in combination, the recorded activities provide an account of the customer's visit to the car dealership. Each AP will compose its observed activities into a collection of blocks and contribute them to the blockchain.

At a minimum, each activity entry included in a block should include tags for the activity itself, the customer, and the AP as well as the activity type, any descriptive details about the activity, and a timestamp. An initial list of supported activity types will be provided, but developers can extend this list arbitrarily for their specific applications or analytics techniques. Examples of activities include:

- ARRIVE: an AP has determined that a customer has arrived at a particular store or location.
- DEPART: an AP has determined that a customer has departed from a particular store or location.
- LOCATION: a customer-side AP is publishing their current location, for use by location-based services.
- BUY: a (customer's or retailer's) point-of-sale AP device indicates that a purchase has been made and includes details of the item purchased, price, buyer, seller, etc.
- SELL: a (customer's or retailer's) point-of-sale AP device indicates that a purchase has been made and includes details of the item sold, price, buyer, seller, etc.
- INTEREST: a customer-side AP can publish a shopping preference, item of interest, or personal preference.
- OFFER: a retailer can publish a short-term offer for discounted items or services, to include an expiration time among other offer details.

Note that some of these activities should appear in pairs (ARRIVE/DEPART, BUY/SELL, etc.), which can be useful as a verification input. This basic format for an activity is shown in the following table, including a description of the field in the right column.

Activity:	<act_tag>	Tag used to reference this activity from elsewhere
Customer:	<cust_tag>	Anonymized tag used to reference observed customer
Observer:	<obsv_tag>	(Possibly anonymized) tag used to reference object, owner, and description of observation source, including metadata as appropriate
Activity:	<activity_type>	Activity type, e.g., ARRIVE, DEPART, BUY, SELL, LOCATION, etc.
Activity details:	<list-of-details>	Details of activity (e.g., what was purchased and for how much)
Timestamp:	<time>	Time that activity was observed (using UTC or similar)

To illustrate the activity data format, we illustrate potential activity blocks that would be created in a retail mall example, noting the contents of the tags without specific protections.

Activity 4E773C91

Customer:	<A>
Observer:	<Mall, store #1, front door camera>
Activity:	ARRIVE
Activity details:	<photo of customer A arriving>
Timestamp:	1496318700 UTC

Activity 36EA9801

Customer:	<A>
Observer:	<Mall, store #1, PoS terminal #3>
Activity:	BUY
Activity details:	<{item: large coffee; cost: $3.50; tip: $1.00;}>
Timestamp:	1496318885 UTC

Activity 7832DAF1

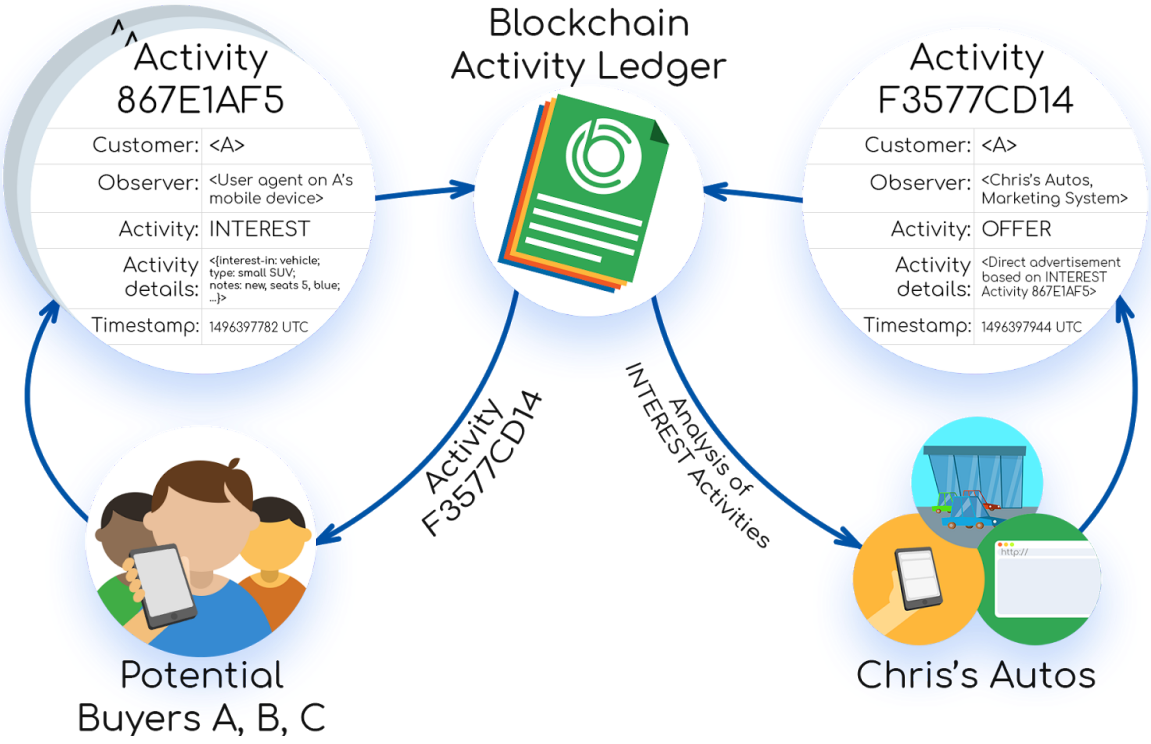
Customer:	<A>
Observer:	<Mall, store #1, front door camera>
Activity:	DEPART
Activity details:	<photo of customer A departing>
Timestamp:	1496318943 UTC

The basic activities (such as arrival time, departure time, and items purchased) already provide useful customer data to the Mall and its current and future customers. In particular, even without knowing the customer's true identity or specific details of the AP or activity (or by replacing these with random numbers in the anonymous ledger), any party can use the activity type and timestamp fields to perform basic retail analytics such as customer count, typical busy hours, or purchases per hour. Other entries and data in the activity block can be encrypted or anonymized to protect identifying information or other sensitive data.

As a simple example of the kind of B2C interaction that the activity ledger enables, we revisit the example given earlier about direct marketing between car dealerships and customers interested in buying new vehicles.

Example: Direct-to-Consumer Auto Marketing

Direct marketing can leverage explicit INTEREST activities created by potential customers, as illustrated below. Retailers can analyze numerous INTERESTs posted on the ledger to identify potential customer matches and create direct-to-consumer advertisements or discounts using OFFER activities. To act on an OFFER that matches a customer's stated INTEREST, they can create a smart contract with the retailer that includes incentives for viewing the ad, visiting the store (e.g., test driving a car), or further interaction retailer-customer interaction. From the retailer's perspective, providing these incentives to the potential customer is likely far less costly with higher return on investment compared to paying an ad service provider.



Customer and Retailer Anonymity In the Activity Ledger

As mentioned above, certain aspects of customer and retailer information stored in the blockchain should be anonymized to prevent identification of customers without their consent, linking sequences of activities to the same customer, or tracking customers and their activities. To discuss the ability to protect against such threats, we rely on the following terminology from the anonymity field.

- In evaluating the level of anonymity provided by these techniques, let's consider the *customer anonymity set*, which is the set of possible customers that a particular block's customer tag could belong to. A larger customer anonymity set corresponds to greater uncertainty around the true identity that a block describes.
- Similarly, we consider the *observer anonymity set* to evaluate the level of anonymity of the relevant retailer that a block describes.
- We use the notion of *linking* and *linkability* between blocks to describe the ability for certain parties to de-anonymize certain tags or to determine that two tags correspond to

the same identity (regardless of the ability to learn the identity). *Unlinkability*, namely the inability to link activities, is closely related to anonymity sets defined above.

- The ability to *identify* a party means that someone can determine the true identity of an entity in the ecosystem (e.g., a public key). Identifiability implies linkability, but not the other way around.

These definitions are in line with the Common Criteria ISO/IEC 15408 standard for Information Technology Security Evaluation.[4]

When an AP posts an activity to the ledger, it is required to use proper anonymity mechanisms to maximize the size of respective anonymity sets subject to any contracts in place with other parties in the ecosystem. The primary mechanism for enabling customer and retailer anonymity is the use of access control groups. In particular, we employ a combination of anonymization and group-based encryption over the customer, observer, and activity detail fields of the individual activities such that the owner of the data can tightly control access to the data and provide unlinkability to entities outside the group. The following example highlights a few key details of identification and tracking, both which we aim to prevent by the general public.

Example: Analyzing customer stay duration

Consider the example Mall activity blocks tabulated above, but now suppose the Mall owner wants to know how long each customer stayed in the store. Computing this customer stay duration requires the owner to link corresponding ARRIVE and DEPART events, as these are otherwise remain unlinkable (unless only one customer is present) if the customer tag is randomized. A straightforward way to achieve this linkability without explicit customer identification (e.g., including the public key of customer *A*) is to have the originating AP encrypt the customer key using a symmetric key *k* as $E_k(A)$, with the understanding that the key is known only to the AP devices comprising the Mall. While this encryption hides the customer's public identity, the result is still static within the context of the store, and every action of customer *A* in this particular Mall could still be linked together by any public entity, though not revealing the identity *A*. To make the activities unlinkable, the AP can include the activity's timestamp (or any other suitably dynamic value) in the encryption as $E_k(A,t)$, so the customer tag appears to change randomly with every instance. The use of a time-dependent encryption (or any other semantically secure encryption mechanism) thus allows the store to link together the customer activities while keeping the details unlinkable for every other party.

Note that in the above example, the APs in the store only know the true identity *A* if allowed per explicit registration or contract with the customer, but any pseudo-identity is sufficient to allow linking within the store and unlinkability outside. Linking across retailers can also be enabled via suitable agreement among parties, as described next.

[4] Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Components, v. 3.1, rev. 4, Sep. 2012, Available https://www.commoncriteriaportal.org/files/ccfiles/ccpart3v3.1r4.pdf.

Group-Based Activity Sharing

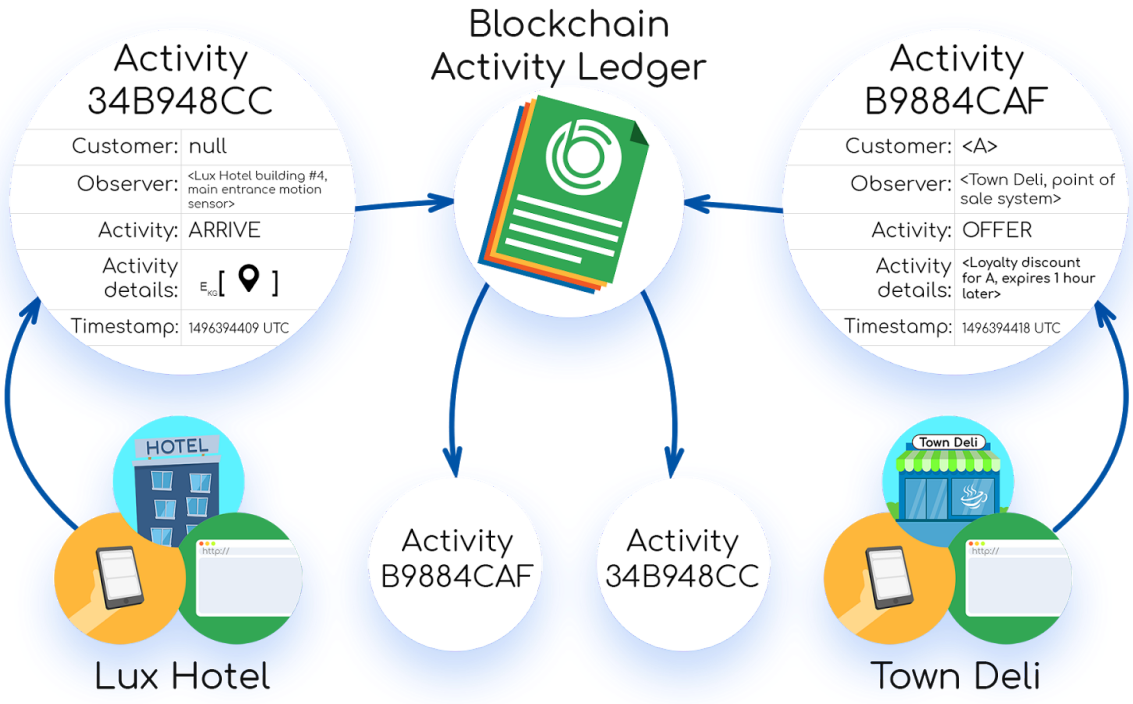
An additional mechanism that can be used to enable and control the ability for private data sharing on the otherwise public blockchain is the use of group-based access control. When an AP creates a new block, it can choose to protect the contents of the block using any number of cryptographic protections or anonymity mechanisms. However, with unlinkability comes a limited value of the data if no other party can access the block contents. With appropriate agreements across organizations, *selective linkability* can be achieved through the use of an appropriate shared credential, namely a group key. By employing group keys with an appropriate mechanism for enrollment/disenrollment in groups, an AP (or its owning entity) can tightly control access to individual fields of a block by using suitable group keys (noting that different group keys can be used to protect different fields / subfields within a block). The following expands the previous example to include the notion of group-based sharing of the details of activity blocks.

Example: Analyzing customer stay duration across multiple stores
Suppose now that a collection of franchises of a Mall chain want to analyze customer stay durations across the different storefronts. Using a similar time-dependent or semantically secure encryption mechanism with a group key *Kg*, the customer and observer tags can be created in such a way as to allow anyone with the group key to perform the required computation. In this case, it may still be beneficial for the different stores to protect the true identity of each customer, which can be done through a straightforward combination of a key *k* shared only among devices within the particular store and the group key shared across stores. This can be done, for example, by creating the customer tag as $E_{Kg}(E_k(A),t))$.

As a more interesting example, the notion of data sharing across groups could also be used to allow multiple independent stores to leverage observations made by each other's respective AP devices. The next example illustrates this new opportunity in detail.

Example: Triggering "Just in time Offers" using nearby AP reports
Activity blocks created by an AP device in one store can be quite useful for direct-to-customer marketing from other stores as well, especially when the stores have contracts for sharing customer activities. Suppose that customer *A* enters a hotel but has no prior relationship with the hotel chain—in this case, an AP can observe *A* entering the hotel but cannot properly identify the customer. The AP creates a new block with activity "ARRIVE", customer tag set to a null value, and activity details, encrypted using the group key *Kg* shared among collaborating stores. Software run by the deli a few doors away from the hotel finds this activity block, uses its group key *Kg* shared with hotel, and identifies customer *A* as a loyal deli customer from the check in information posted by the hotel. The deli's point of sale system can initiate a just-in-time "OFFER" activity to customer *A* with a direct-to-consumer advertisement or discount offer, using credentials from their previous relationship and the knowledge that *A* is at the nearby hotel. This opportunity can be attained without requiring each store to have an app on

the user's mobile device and without requiring user location tracking. This example demonstrates the added value of collaboration across organizations using the public blockchain.



In general, the notion of groups is highly customizable by the entities in the marketplace, as anyone creating activity data can serve as a group manager, and any other party can negotiate to become a member of a group, using an appropriate smart contract between parties.

Activity Analytics and Verification

As discussed, the main value of the anonymized activity ledger is the ability to share anonymized customer and retailer data to facilitate analytics that provide value to customers and retailers in the ecosystem. While the specific AP controlled by the customer or retailer has some control over the protection of data in the individual activities they contribute using group-based protections, there are incentives to sharing certain data entries publicly or with less protection. Before discussing specific incentive mechanisms in the next section, we first highlight several analytics capabilities that are enabled by the activity ledger.

- Access to certain details of a BUY activity can be used to analyze purchasing trends, identify items in high demand, or expose similar patterns. Again, rather than publishing such details publicly, access can be controlled cryptographically using group key management, encrypted search, or other techniques.

- Detection and analysis of customer activity sequences that contain ARRIVE and DEPART activities with no intermediate BUY activity can be used to understand customer behaviors about shopping trips that did not result in a purchase. This data could create an opportunity for a retailer to offer a discount on relevant products to the shopper. In addition, by analyzing AP data across online and physical stores, retailers can get a better understanding of how customers learn about products before making a purchasing decision, possibly uncovering patterns in customer loyalty to specific retailers.

In addition to activity analytics for the purpose of opportunity identification and prediction, parties can use the data from the activity blockchain to verify claims (analogous to forensic evidence), for example to satisfy the conditions of a smart contract made with another party in the ecosystem. For example, if a retailer and a customer create a smart contract stating that the retailer will pay the customer some fixed amount for attending an in-store event, then the retailer may rely on data contributed to the activity ledger from several other parties as evidence or proof that the customer fulfilled their obligations. Such verification is highly relevant to the discussion of smart contracts in the next section.

Token-Driven Ecosystem

The narrative revolving around the anonymous activity ledger relies on the assumption that customers, retailers, and third-party entities will contribute activity data to the system. In addition, the system relies on the assumption that parties will take action to participate in the smart contract process with each other. To satisfy these requirements, we are driving the ecosystem with the creation of a BitClave Consumer Activity Token (CAT) to incentivize bootstrapping of the ecosystem and continued participation and interaction in the ecosystem. In what follows, we describe three main aspects of the token-driven ecosystem built around the CAT, which can be exchanged in arbitrary fractional amounts.

Tokens as Incentive for Participation

As the basis for retail analytics, customer activity prediction, and activity verification, the richness of data contributed to the activity ledger is a key priority. As such, all data contributed to the ledger will be rewarded with CATs, awarded to the owner/operator of whichever AP contributes the data, independent of their involvement in the activity itself (meaning a third party “witness” can contribute data and receive a CAT reward). The precise amount of CATs awarded to the contributor must be sufficient to incentivize data contributions, which is a function of the market value of CATs, discussed in a later section. In addition to tracking the value of CAT itself, the system supports dynamic incentive pricing, meaning that the amount of CATs awarded for contributing can vary independently of the CAT value, like any commodity good. One example of a practical requirement for dynamic incentive pricing is AP traffic traffic normalization such that the CAT value is relative to the overall value of an AP's audience and traffic. For example, scale has to be normalized so that larger retail destinations are indexed properly against

smaller, but potentially more valuable traffic. Because the CAT is awarded to the owner of a contributing AP, every activity must be strongly bound to such an identity. This is part of the reason why every activity must include an AP tag that identifies the originating party, which if anonymized must be linkable to the entity providing the CAT rewards. Activities posted with no such linkable tag (from the perspective of the incentive provider itself) will stay in the blockchain but will not incur any reward.

In addition to incentives for contributing data, entities can choose to provide additional incentives for performing certain types of activities, though not necessarily bound by a contract. For example, a retailer can offer customer incentives for registering or opting into their loyalty rewards program (which is controlled by a suitable group key), shopping in the store by providing a reward to any (registered) customer who visits, or by agreeing to view sponsored content.

The particular incentive amounts and relative value of contributing different types of activity data to the ledger will be determined after further study of the market economics of the system.

Smart Contracts for Activities

Once the BASE blockchain is populated with sufficient activity data, the further role of the CAT is to facilitate execution of smart contracts among parties in the ecosystem. In particular, any two parties can create a smart contract detailing a prescribed set of activities to be executed. Here are a few examples:

- Customer registration with a retailer, such as a loyalty rewards program, can be facilitated via smart contract. Such a contract provides an incentive for the customer to allow the retailer to contribute anonymized data on their behalf or to identify or link their activities within the retail environment.
- A retailer and a customer can create a smart contract indicating that the retailer will reward the customer a fixed amount of CATs for attending a product demo. Such a contract would likely be informed by the customer's shopping history and preferences.
- Contract to exchange CATs for purchase coupon from retailer, equivalent to using CATs for purchase.
- "Witness Request": parties can negotiate contribution of specific additional data not previously contributed to the ledger for a non-market price, to facilitate verification of other contract terms or for other purpose. For example, an AP can issue CAT payment to an entity providing data that supports verification of activities required for another contract (i.e., acting as a proxy AP or witness to an activity). In this case, any responding party would be required to coordinate with the requestor to facilitate posting the content privately and anonymously, as described above.

As described previously, activity data contributed to the activity ledger will be used to determine successful execution of the contract and subsequent CAT reward.

Retail Analytics Providers

The unique nature of the BitClave Ecosystem introduces a new role beyond those of the standard customer and retailer. Since the smart contract landscape requires significant information harvesting and analytics capabilities based on the activity ledger, entities can take the role of an *analytics provider*. In this role, an entity can create and sell custom analytics capabilities in the BitClave ecosystem, effectively extending the market to include services as well as retail goods. As such, a retailer who wants to know a particular feature of their customer base can create a smart contract with an analytics provider to create the desired functionality. While the ecosystem does not explicitly support contracting and bidding processes, any developer or organization could create this possibility by introducing new activity types and associated mechanisms for bidding and negotiation.

Deployment Plan

Combining the above components, the BitClave Activity Search Ecosystem acts as a platform for creating customer-driven and incentivized retail opportunity. As the platform provider, BitClave's primary focus is to establish the core framework of the ecosystem, upon which all developers can create apps and services. In one sense, the BitClave platform is to the retail ecosystem what Facebook is to social networking. As such, BitClave's core offerings to support the B2C ecosystem (as well as B2B support services) will include a core application (browser and app based) and a collection of APIs, libraries, and SDKs that will allow external developers to build on top of the platform (analogous to the Facebook Graph API). In another sense, given an open platform with no established intermediary, BitClave offers similar services and derives revenue in the same way as any third-party developer within the ecosystem. BitClave apps benefit from first-mover advantage as well as tight integration with service providers across the ecosystem but in a decentralized platform it is plausible and well rewarded for developers and service providers to "out BitClave" BitClave.

Initial Development Efforts

The initial design of the platform will be based on the INTEREST and OFFER activities described previously. We envision a mobile app (as the user's primary AP) with a "search engine" interface that allows users to create INTEREST activities by initiating a search request for a particular service or product. Retailers and service providers who can fulfill the user's interest request can submit OFFERs to the customer, with an appropriate payment incentive for them to view and/or respond to the OFFER.

We will then gradually include further activity creation capabilities into the mobile app such as browsing an online retailer or checking into a particular offline storelocation (i.e., creating ARRIVE and DEPART activities) and initiating purchases with retailers or other users (i.e., creating BUY and SELL activities).

Value and Experience for Early Platform Users

While the true value of the ecosystem will take time to attain, reaching a sufficient number of retail contributors and user participants, we believe there is sufficient value for early adopters of the retail platform. Initial users can start to earn CATs by creating profile details, contributing preference and interest data, and posting recommendations for retailers or providers who have not yet joined the system (potentially earning tokens and reputation from other users in the process) similar to a recommendation or referral system. From the outset, the platform will support peer-to-peer contracts which will provide value in bootstrapping the retail marketplace.

Once the platform is launched, team BitClave will shift significant focus to marketing to small and medium businesses to build the retail side of the marketplace, with the expectation that more retailers will bring more customers, leading to continued growth of the ecosystem.

Growth Plan

As part of the initial ecosystem bootstrapping, we will target industries where significant effort is put into marketing to individual customers, such as auto sales, real estate, hotels, and retailers like Target that compate with major ad service providers like Amazon. We are already in early discussions with several medium-to-large size retailers and hotel chains, which would give us access to customers in thousands of properties around the world.

New Opportunity

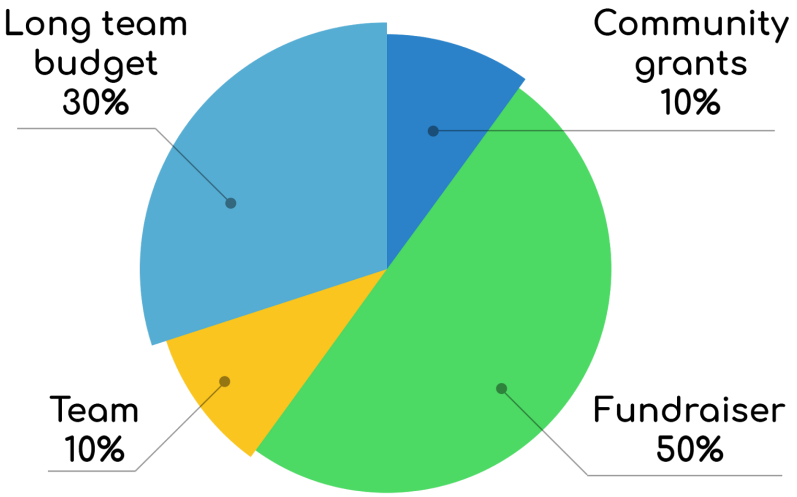
BitClave designs and develops a open source decentralized search ecosystem, upon which external developers create apps and services. The core offering includes the framework enabling external developers to build on top of the platform.

Initial participants will earn CATs by contributing consumer data (e.g., profiles, interests), transactions, and referrals.

Fundraiser and Token Distribution

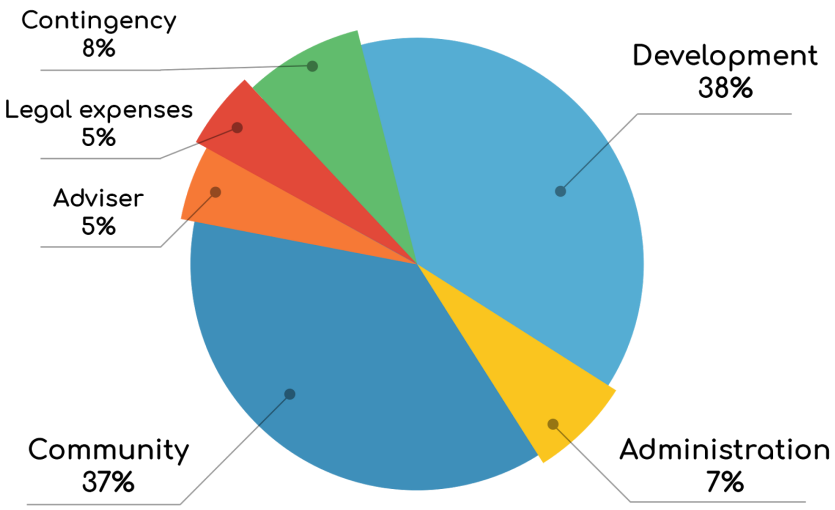
Details will be announced soon.

Community grants: 10%
Team: 10%
Long-term budget: 30%
Fundraiser: 50%



Use of Proceeds

- Development: 38% of budget. This financing allows for the rollout of the solution, including the necessary adjustments.
- Administration: 7% of budget. Consists of associated administration costs.
- Community: 37% of budget will focus on expanding adoption. This also includes the growth and maintenance of the world-wide community.
- Advisers: 5% of budget. These funds will be directed at growth-hacking, PR, partnerships, affiliate programs and more.
- Legal expenses: 5% of budget.
- Contingency: 8% of budget. This is a set-aside for unforeseen costs.



Fundraiser Schedule

Official dates and discount schedules will be announced in the coming weeks.

Benefits to Users

Users will be given a corresponding amount of CATs at the initial exchange rate specified above. Since the total volume of CATs is fixed, token exchange among the growing population of retail partners and customers implies a general growth model for CAT value. In particular, as more retailers and customers join the BitClave Ecosystem, quantity and quality of activity data contributed to the ledger will gradually improve, meaning the per-contribution reward will decrease, corresponding to an increased CAT value. Similarly, at more service providers join, the amount of CATs required for an equivalent service will gradually decrease, corresponding to a similar CAT value increase. Overall, we expect the CAT market value to stabilize based on an implied minimum cost of operating as a service provider and minimum incentive for participation.

Roadmap

PRE MILESTONE 1.0
BitClave has a functioning Activity Ledger that allows user registration and keeps user activity, utilizing an anonymizing algorithm to preserve user-privacy. BASE allows businesses to create smart contracts to automatically display special offers and products based on user activity.

MILESTONE 1.0
The BitClave ecosystem allows for the creation of search-based mobile applications, as well as well as access to the broader BASE ecosystem. This access allows users to search for products and services to collect anonymous user activity in order to perform smart contracts. Businesses can modify both smart contracts and their intended purposes to best-suit their needs. An auction algorithm controls the volume of offers.

BEYOND MILESTONE 1.0
BitClave provides a built-in wallet to control the flow of CATs distributed on Ethereum, utilizing a state channel scheme with Zero Knowledge Proof protocol to ensure user privacy. Partners build applications on the BitClave infrastructure, creating, modifying, and accessing smart contracts and data in the BASE ecosystem. BitClave completes partnership with a gateway to payment systems with hundreds of millions of users, ensuring integration with all users of the payment system as well as resulting in improved standards and resource for new business entrants. Concurrently, BitClave completes strategic collaborations with retailers on proof of concepts and product releases showcasing seamless customer registration and rewards programs that integrate with BASE.

Team

BitClave was founded in 2016 with the vision of reimagining the relationship between businesses and customers based on the trust and transparency of Smart Contracts. Our solution has the potential to disrupt one of the largest markets in the world, the ad network, which is currently monopolized by giant corporations and controlled by middlemen.

People and governments around the world have concerns over personal privacy. Much of this concern is attributable to the bait-and-switch model of "free services" dealing in privacy-invasive data mining practices.

These practices are justified due to the business economy they are purported to support, but instead contribute to a disjoint promotions and purchases continuum where businesses pay a high price for metrics with little correlation to direct sales while diverting significant resources from quality, loyalty, and value building.

At our best, we foster the social accountability and service oriented qualities of the local economy with a decentralized and open handed approach to market engagement.

For BitClave, the world is a better place if the hidden ad networks are transmuted and elevated into an activity-driven marketplace where customers and brands, alike, share in value creation while fostering meaningful relationships bridging promotions and purchases.

EXECUTIVE TEAM
BitClave currently has a partnership with a gateway to payment systems with hundreds of millions of users, which will ensure integration with businesses entering the market.

The team consists of 20 engineers and the advisory board of world-class talents in the fields of security, payments, and blockchain.

CEO
Alex Bessonov
Senior Executive with over 20 years of experience in the security, privacy and blockchain industry. Former CSO of LGE.

CTO
Patrick Tague
Associate Research Professor in the ECE Department at CMU. Expert in mobile, embedded, and wireless security.

Chief Architect

Emmanuel Owusu
PhD from CMU. Expert in the fields of security, blockchain, Internet of Things, public policy and privacy.

Project Management
Vasily Trofimchuk
MSc in CS, MBA. A serial entrepreneur. Expert in advertising, game theory, blockchain and management.

Head of Marketing
Min H. Kim
Marketing & Partnerships at Draper University. Dartmouth alum, venture debt, and early-stage operating experience.

Security Architect
Yan Michalevsky
PhD from Stanford. Entrepreneur, expert in computer systems, software security and privacy.

Core Developer
Andrey Shashlov
Full stack developer with focus on Android and iOS. Entrepreneur and innovator. Blockchain enthusiast.

Data Architect
Eugene Kaganovich
Full stack developer with deep knowledge of Java. Expert in protecting enterprise data in the cloud.

Data Scientist
Mark Shwartzman
MSc from University of Tel Aviv. Expert in video compression and data science. Bitcoin enthusiast and developer.

EXPERT ADVISORS

Blockchain Advisor
Danny Yang
PhD from Stanford. Expert in cryptocurrencies and blockchain. Founder of MaiCoin and Blockseer.

Blockchain Advisor
George Samman

Blockchain enthusiast and entrepreneur. Former cofounder of Magnr and contributor to CoinTelegraph.

Governance Advisor
Gerald Beuchelt
CISO at LogMeIn. Former CISO at Demandware. A member of the Infragard Member Alliance Boston Chapter Board of Directors.

Strategy Advisor
Kevin Doerr
Microsoft, Yahoo, Weather.com and GoDaddy executive. Expert in user experience, security and team building. Angel investor.

Data Privacy Advisor
Balaji Ganesan
Serial entrepreneur. CEO of Privacera. Expert in data privacy and security. Focused on GDPR compliance.

Technology Advisor
Charlie Liu
Head of Global External Innovation & Partnership at Sony Mobile Communications. Technology expert.

Risk Advisor
George Totev
Head of Risk and Compliance at Atlassian. Global Security Leader with expertise in governance and risk management.

Science Advisor
Brad Gaynor
PhD in EE, Tufts University. Founder and CTO of Lexumo, Built the Cyber Systems Business at Draper Laboratory.

Legal

We will publish the Terms of Sale and company incorporation information a week before the crowdsale starts.

Glossary

Activity: an action observed and recorded by an Attestation Point. Activities include both in-person actions (e.g., visiting a retail store or buying a product) and online actions (e.g., rating a retailer via a mobile application or using a coupon code in an online purchase). Activities may be associated with customers, businesses, or both (see The Anonymized Activity Ledger).

Attestation Point (AP): a software and/or hardware sensing module that records customer activities to the activity ledger. Some examples of APs include mobile devices, cameras, apps, cloud servers, WiFi routers, and Bluetooth hubs (see Technology Overview).

Anonymized Activity Ledger: a decentralized account of relevant customer and retailer activities using anonymization and unlinkability technologies (see The Anonymized Activity Ledger).

BitClave Active Search Ecosystem (BASE): refers to the entire suite of protocols that define the platform for decentralized attestation and search of activity data (see Technology Overview).

Consumer Activity Token (CAT): the token that underlays all transactions among participating parties. These tokens are used as a form of rewards for the variety of services available within the Retail Activity Market (see Token-Driven BASE).

Retail Analytics Provider: an entity that sells analytics capabilities (see Retail Analytics Providers).

Selective Linkability / Unlinkability: group-based access control can be used to control which parties are able to link activities to a common (though possibly unknown) identity (see Group-Based Activity Sharing).

Smart Contracts: an automatically enforced agreement among two or more parties in the ecosystem mapping a set of activities to ledger operations to be executed (see Smart Contracts for Activities).

Token Exchange: a community established exchange rate, assigning value to a given activity or service (see Tokens as An Incentive for Participation).