BitClave
Decentralized Search Ecosystem

Distributed Blockchain-Based Smart Contracts for Connecting Consumers and Businesses

http://www.bitclave.com

Draft v 0.7.5

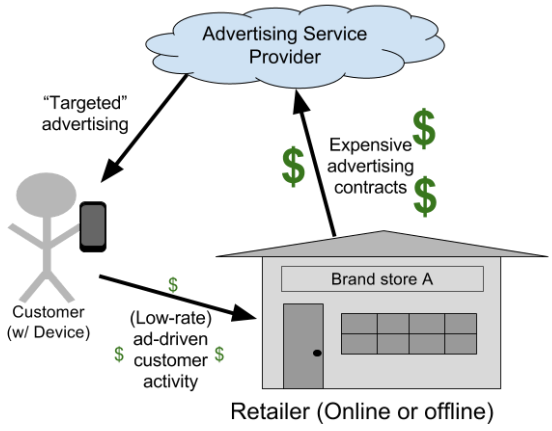
June 2017

Problem Description and Solution

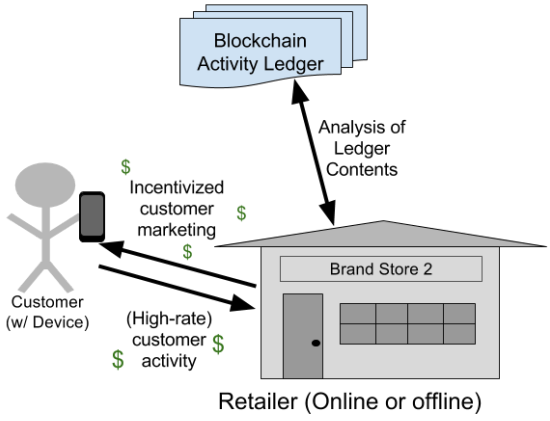
Simply put, advertising — a market worth nearly 550 billion dollars — is broken.[1] When it comes to online advertising, businesses, in order to get their advertisement content online, are forced

[1] Statista, "Global Advertising Market - Statistics & Facts", Available https://www.statista.com/topics/990/global-advertising-market/, accessed June 15, 2017.

to pay “middlemen” exorbitant amounts of money to reach a captive audience of users for their promotions. However, their promotions often find themselves among many other ads clogging up space on crowded banners, or simply ending up in someone’s spam box. Businesses also have little to no guarantees that the traffic they generate on their promotions is genuine — in fact, nearly 50 percent of all advertising traffic is generated by bots [2, 3], essentially defeating the purpose of advertising itself. Offline advertising is a similar story — more often than not, offline advertisers promote content with a “hit or miss” mass mailer mentality. Hoards of content are slammed into users faces, with little to no targeting present resulting in a dubious correlation between offline ad dollars and return on investment. This, along with other factors, contribute to the extremely low conversion rates and, as promotions are largely delivered to those who simply do not care for the product or in contexts where user attention is likely elsewhere. 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, Facebook, and others, the more money consumers have to pay for the products. Businesses end up losing money and consumers end up paying more for less value, creating a lose-lose situation.



(a) Traditional advertising services: retailer pays high cost to advertiser, advertiser serves large number of somewhat-relevant ads, small number of customers respond to ads.



(b) Decentralized blockchain-based marketplace: retailer analyzes activity ledger to determine target customers, approaches customers individually, higher number of customers respond.

In order to counteract these problems, BitClave proposes a system in which these intermediaries are eliminated. Instead of paying any “middlemen”, companies automatically make personalized offers directly to consumers who have opted in for the service, as illustrated above. 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. Not only does this ensure that companies are making their offers to an audience that is more inclined to view and interact with the product, it also allows consumers to earn money for viewing these promotions. This also provides for increased user privacy — ”free” services, such as Google and Facebook, often sell user data to brokers. With the BitClave Ecosystem in place, however, this is no longer a concern as companies sell their promotions to consumers firsthand.

Sample Business Use Case

The BitClave system is applicable to any space — offline or online. ; however, for illustrative purposes, the following sample use case describes how the system may be applied to the auto industry.

For every customer lead, car dealers spend up to $200 in order to spread the word through advertisements on Google, as well as other forms of advertising such as banners around the city. In the BitClave Ecosystem, however, the dealership will have the opportunity to display their promotions and advertisements directly to a potential buyer, utilizing the precise targeting that our system 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. Given access to ratings, the business, for instance, will be aware if the consumer has taken up a high volume of promotions before, but had never followed through and thus not likely to purchase in the future. Similarly, analysis of a given customer's activity over time enables businesses to identify customers who have shown 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 the business 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.

Overview of the BitClave Retail Activity Market

BitClave is a startup company, based in Mountain View, California, providing innovative automated customer recognition solutions and seamless payment methods for use specifically in the retail, hotel, restaurant, and other small to medium size businesses.

One of the primary innovations that BitClave is focusing on is a distributed blockchain-based system, called the **BitClave CAT ecosystem**, which would allow storing and managing vast amounts of data consisting of records of customer activities from an unlimited and variegated number of **Activity Observation Sources**. Examples of such customer activities would be

entering a particular building, accessing a particular WiFi network, making a purchase, opening a mobile app, and requesting a delivery online. These activities can include anything that can be observed and automatically processed by specifically enabled activity observation sources, such as cameras, mobile devices, apps, cloud servers, WiFi routers, and Bluetooth hubs. **Instead of selling this data to monolithic advertising service providers, the collected data would be contributed in a decentralized manner using blockchain,** similar to the way Bitcoin is implemented.

Each block posted into the blockchain contains anonymized information about a particular observed 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 would 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.

On top of this distributed activity data collection system, BitClave is introducing a form of cryptocurrency, 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 the BitClave Retail Activity Market would make possible. The CAT-based market puts much more power into the hands of the 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 data and message posts on the public blockchain, and additional parties can contribute as service providers by creating analytics capabilities that operate over the data in the blockchain.

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 a more direct access to interested customers and a more measurable correlation between promotional expenses, customer activity, and return on investment.

BitClave's Retail Vision and Value Statement

We believe that a blockchain-based system is ideally suited for 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** 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 will be 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 will contain encrypted data that is only available to specific groups. 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 cryptocurrency-driven **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.

The Anonymous Activity Ledger

The anonymous activity ledger is the foundation of our retail ecosystem, providing a decentralized capability for crowdsourcing and sharing data about the activities of customers and retailers. The ledger allows a wide variety of analytics capabilities that leverage the broadly collected yet anonymized data from customers, stores, and websites across different retail domains. As mentioned previously, any party who can observe activities in a retail domain — whether store, customer, or 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, depending of course on access to protected data and loyalty program or contract-based agreements with 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 *activity observation source (AOS)*, noting that an **AOS could exist in either the digital or physical domain**. Examples of AOSs include video cameras, mobile devices/apps, wireless network elements (e.g., WiFi access points, Bluetooth beacons), point of sale terminals, landing pages on retail websites, http redirects, and so on. Note that many of the AOS 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 AOS is capable of creating data entries to the ledger, but only those AOSs owned by the customer or by an entity with an existing relationship (e.g., service registration, loyalty program, smart contract) with the customer will be able to include (encrypted) information about the customer's identity. Retail AOS devices 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 a video

camera deployed by a coffee shop owner, aimed at the front entry door. The camera can be pre-programmed with the identifiers of the coffee chain and the specific store, but it will not be able to identify individual customers. However, if the camera is integrated into the coffee shop's customer loyalty database, then facial recognition software can be employed to recognize customers who have opted into the program and contractually allowed the coffee shop to include their anonymized identity information into the activity report. Customers who have not opted in cannot be identified by the AOS, so the activity report will not include any customer identity in this case. Independent of the identification of the customer, the coffee shop camera or system can identify specific activities including customer arrival, departure, and browsing items for sale. 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 coffee shop. Each AOS 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 AOS 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 AOS has determined that a customer has arrived at a particular store or location.
- DEPART: an AOS has determined that a customer has departed from a particular store or location.
- LOCATION: a customer-side AOS is publishing their current location, for use by location-based services.
- BUY: a (customer's or retailer's) point-of-sale AOS 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 AOS device indicates that a purchase has been made and includes details of the item sold, price, buyer, seller, etc.
- INTEREST: a customer-side AOS 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 the coffee shop example above, noting the contents of the tags without specific protections.

Activity 4E773C91	
Customer:	<A>
Observer:	<John's Coffee, store #1, front door camera>
Activity:	ARRIVE
Activity details:	<photo of customer A arriving>
Timestamp:	1496318700 UTC

Activity 36EA9801	
Customer:	<A>
Observer:	<John's Coffee, store #1, PoS terminal #3>
Activity:	BUY
Activity details:	<{item: large coffee; cost: $3.50; tip: $1.00;}>
Timestamp:	1496318885 UTC

Activity 7832DAF1	
Customer ID:	<A>
Observer:	<John's Coffee, store #1, front door camera>
Activity:	DEPART
Activity details:	<photo of customer A departing>
Timestamp:	1496318943 UTC

* <x> denotes that the content x is masked or protected in some way (e.g., encrypted or hashed)

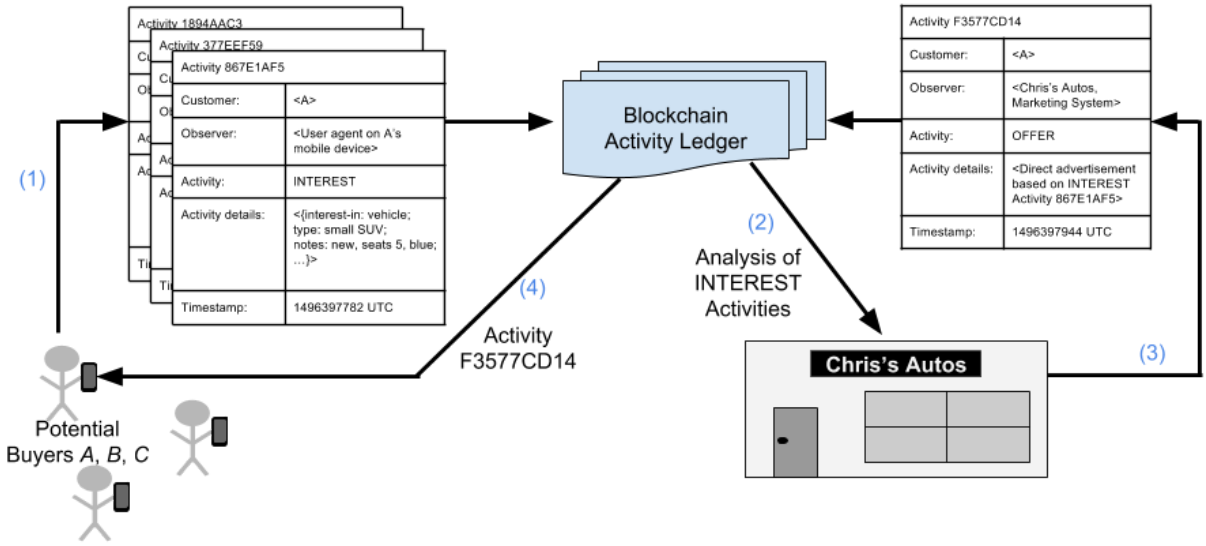
The basic activities such as the examples above already provide useful customer data to the coffee shop and its current and future customers. In particular, even without knowing the customer's true identity or specific details of the AOS or activity (or by replacing these with random numbers in the anonymous 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 an interested 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 our ability to protect against such threats, we rely on the following terminology from the anonymity field.

- In evaluating the level of anonymity provided by our techniques, we 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 larger 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.[2]

[2] 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.

When an AOS 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. Our 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 coffee shop activity blocks tabulated above, but now suppose the coffee shop 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 would 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 AOS encrypt the customer key using a symmetric key *k* as $E_k(A)$, with the understanding that the key is known only to the AOS devices comprising the coffee shop. 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 coffee shop could still be linked together by any public entity, though not revealing the identity *A*. To make the activities unlinkable, the AOS 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 AOSs in the store would 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.

Group-Based Activity Sharing

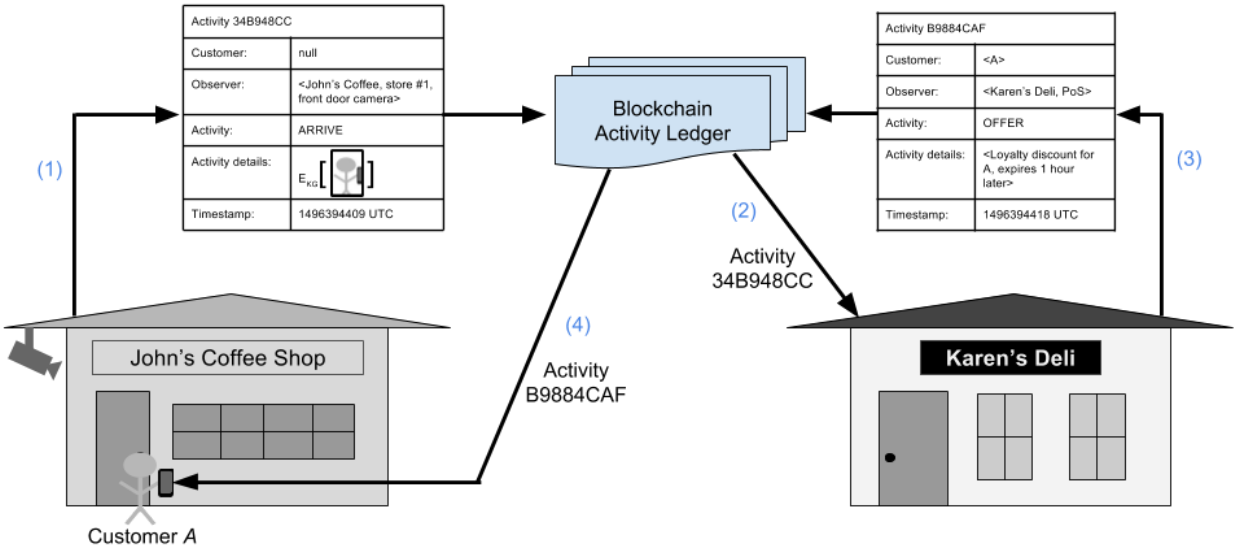
An additional mechanism that can be used to enable and control the ability for private data sharing on the otherwise public blockchain is the use of group-based access control. When an AOS creates a new block, it can choose to protect the contents of the block using any number of cryptographic protections 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 AOS (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 coffee 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 AOS devices. The next example illustrates this new opportunity in detail.

Example: Triggering "Just in time Offers" using nearby AOS reports
Activity blocks created by an AOS 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 John's Coffee but has no prior relationship with the store -- in this case, a camera pointed at the front entry can observe *A* entering John's Coffee but cannot identify the customer as *A*. The camera AOS creates a new block with activity "ARRIVE", customer tag set to a null value, and activity details including a camera image of the customer, encrypted using the group key *Kg* shared among collaborating stores. Software run by the Karen's Deli store just a few doors away from John's Coffee finds this activity block, uses its group key *Kg* shared with John's Coffee, and identifies customer *A* as a loyal Karen's Deli customer from the image posted by the camera at John's Coffee. Karen's Deli can initiate a just-in-time "OFFER" activity to customer *A* with a direct-to-customer advertisement or discount offer, using credentials from their previous relationship and the knowledge that *A* is nearby at John's. 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 anonymous 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 AOS 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 our 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 AOS 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.

- *[more examples to be added]*

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.

A Token-Driven Retail 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 An 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 AOS 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, our 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. Because the CAT is awarded to the owner of a contributing AOS, every activity must be strongly bound to such an identity. This is part of the reason why every activity must include an AOS 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 Retail Activities

Once the BitClave ecosystem 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 would provide an incentive for the customer to allow the retailer to contribute anonymized data on their behalf or to identify/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, I'll pay X CATs for someone to post a picture of person Y at event Z. 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 our 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.

BitClave B2C Ecosystem Deployment Plan

Combining the above components, the BitClave B2C Ecosystem acts as a platform for creating customer-driven and incentivized retail opportunity. As the platform provider, our primary efforts will be to design and develop the core framework of the ecosystem, upon which external developers can create apps and services. In essence, the BitClave platform is to the retail ecosystem what Facebook is to social networking. As such, our core offerings to support the B2C ecosystem 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).

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 AOS) 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 our retail platform. Initial users can start to earn CAT token 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, our team 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 our 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.

BitClave ICO and CAT Distribution

Conversion Rate: 1 ETH = 100 CAT
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.

BitClave ICO Schedule

The fundraiser will run for 30 days or until the hidden cap is reached, with a 1 day minimum time. Cap will be revealed when 80% of the cap is reached.
Official dates and discount schedules will be announced in the coming weeks.

Benefits to Investors

Investors 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 CAT 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.

Legal and Company Incorporation Information

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

Glossary

Activity: an action recorded by an Identifying Source. 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 Public Activity Ledger).

Activity Observation Sources: a software and/or hardware sensing module that records customer activities to the Retail Activity Market. Some examples of activity observation sources include mobile devices, cameras, apps, cloud servers, WiFi routers, and Bluetooth hubs (see Overview of the BitClave Retail Activity Market).

Anonymous Activity Ledger: a decentralized account of relevant customer and retailer activities (see The Anonymous Activity Ledger).

Consumer Activity Token: the cryptocurrency 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 A Token-Driven Retail Ecosystem).

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

Retail Activity Market: an encrypted and distributed blockchain that supports the storage, management, and release of customer activity records collected at Identifying Sources (see Overview of the BitClave Retail Activity Market).

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 Retail Activities).

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

References

[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.
[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.