BitClave

Active Search Ecosystem

WHITEPAPER, ver. 0.9.10, December 2017

http://www.bitclave.com/

In the current $550B ads market, too much money goes to the hidden ad network with too little added value for businesses and customers. BitClave is using blockchain to eliminate ad service “middlemen” and create a direct connection between businesses and customers.

On the **BitClave Active Search Ecosystem**, customers control their identity, decide who has access to their data, and are “paid” each time businesses “use” their data to make them offers.

With BitClave, businesses have a direct relationship with customers and can offer a uniquely targeted promotion. With BitClave, an open search marketplace keeps prices fair, and elimination of intermediates brings all value to customers and businesses.

Content

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, with only a 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 such as overwhelming volume, 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. As companies are forced to pay increasing amounts to “middlemen”, such as Google and Facebook, a direct consequence is higher price markup that 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 these problems, 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 based on their explicit search for goods and services using BitClave's decentralized search application.

In the BitClave ecosystem, consumers have control over their own data and can choose whether to reveal their identity or personal information to retailers as part of their search. At the same time, retailers respond to these searches with targeted promotions, which consumers are compensated for viewing. The resulting market may incentivize consumers to share some personal information, but this type of sharing is not required for successful search. The ecosystem enables users to control their own privacy preferences, unlike “free” services like Google and Facebook, who often sell user data to brokers.

With the BitClave Active Search Ecosystem in place, selling data is a thing of the past, as companies offer promotions to consumers firsthand, creating an efficient and rich market economy among consumers and retailers.

Problem Description

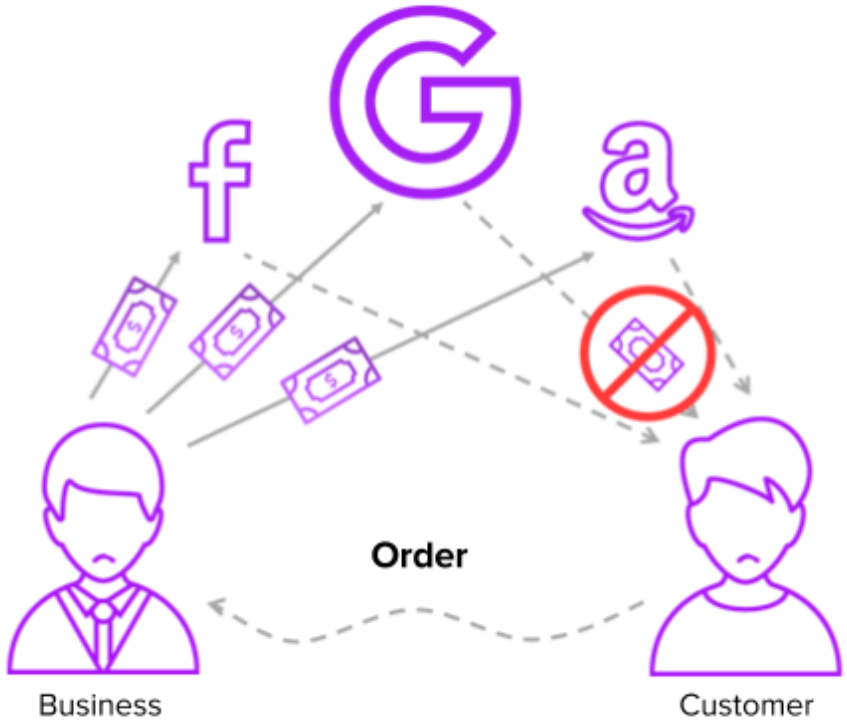


Figure 1: In the current advertising ecosystem, businesses are forced to pay huge amounts of marketing capital to advertising "middlemen", who weakly target customers but provide little-to-no direct value to the customers they advertise to. For customers and businesses, this is a lose-lose scenario, while the advertising giants get rich in the process.

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 businesses trying to find customers. Businesses receive no guarantee that 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[2]. The more businesses pay for

[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.

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 the lose-lose situation captured in Figure 1

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 maximize their own profits by increasing the price of desirable ad placements and click-through 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 Consumer 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[3] and the General Data Protection Regulation (GDPR)[4] in the European Union (EU) highlight the emerging trend of governments forcing technology companies to build-in consumer privacy by design.

It is well known that actionable customer data has intrinsic value. Allowing customers to control their own data and providing incentives for them to share their data in a controlled, privacy-respecting way using blockchain creates new opportunities for customers while respecting regulations.

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

[3]See, for example, the draft proposal to update the ePrivacy Directive, available at https://ec.europa.eu/digital-single-market/en/news/proposal-regulation-privacy-and-electronic-communications.
[4] EU General Data Protection Regulation (GDPR), http://www.eugdpr.org

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. 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 has 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 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 rich knowledge and social structure—follow a very similar business model dating back to before Yahoo and the yellow pages. As the goal of online advertising is to connect business with relevant customers, service providers and business spend significant portions of their marketing budgets on ad impressions, page views, and click-throughs. This approach only loosely translates to business sales or customer value. This is largely due to the combination of popular “free” web services and the murky web of hidden ad networks, resulting in a wide and costly gulf between the two parties. We argue that the advertising model of the "middleman" is not only unnecessary but potentially detrimental to business value and reputation.

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. 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. Decentralized search is the next step in this progression of advertising as a medium for people and businesses to connect. BitClave applies these powerful design patterns to reimagine a more transparent and meaningful medium for people and businesses to engage in value creation.

With decentralized search, previously wasted ad dollars are redirected to promotions that reach customers who are genuinely interested in the products being sold and rewards programs that are truly suitable for customer desires. With a well-devised blockchain system, customer profiles can be elevated from shadowy privacy-invasive metadata, owned and controlled by third parties, into search metadata owned by customers and selectively revealed only when relevant to the search, creating a privacy-friendly marketplace where customers and businesses share in value creation. By storing customer data in a protected way on the public blockchain (i.e., providing anonymity and selective data sharing), new forms of rewards and loyalty programs can emerge.

The advertising industry is once again ripe for technology-enabled disruption. BitClave technology enables 1) scalable search over huge datasets; 2) data privacy and customer anonymity; and 3) incentives to participate in the advertising market.

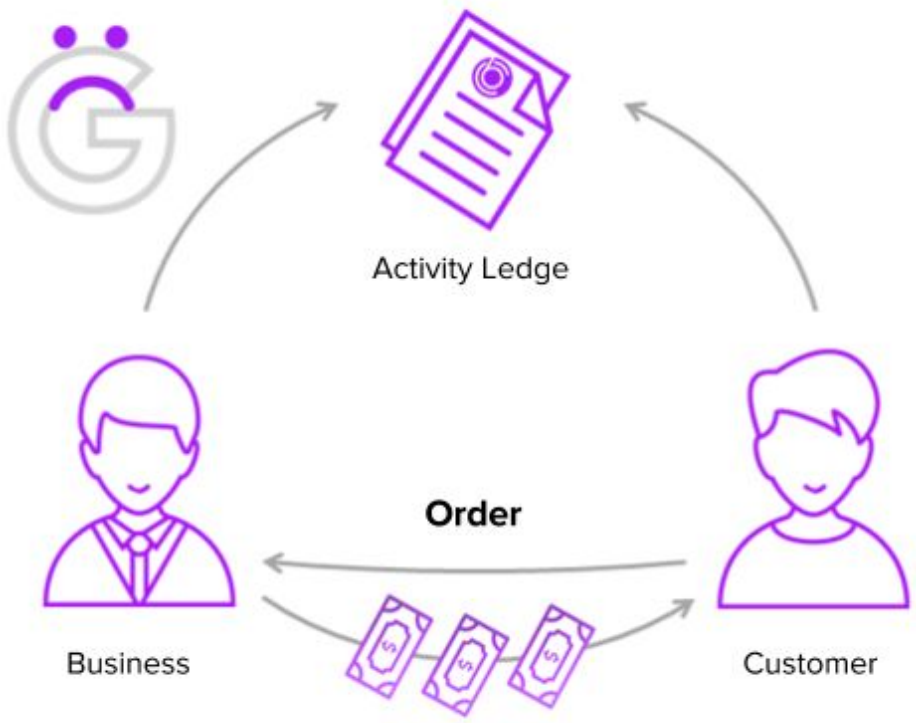


Figure 2: In the BitClave Active Search Ecosystem (BASE), businesses directly market to customers whose searches align with the goods and services being offered. Customers can earn CAT tokens for interacting with directly targeted ads, while businesses get stronger customer leads. The entire matching process is facilitated through the BASE activity ledger, which protects private customer data and allows selective data sharing.

Solution Description

Bitclave's Decentralized Search Ecosystem Realizes Unparalleled Market Efficiency Across The Customer-to-business Value Chain

The vision of decentralized search is achieved by supporting distributed, customer-driven collection of customer activities on the blockchain. Using online data collected in an *anonymized activity ledger* as well as

profiles and preferences that are posted and maintained by customers directly, BitClave is creating a token-based ecosystem for demand-driven marketing and retail with a low barrier to entry for all parties. This ecosystem utilizes the strengths of traditional online advertising, the widespread ability to generate and share user data and the far reach of the internet, but removes the hurdles traditionally present in the digital ad space, namely privacy infringement, untrusted sources of data, and expensive third-party ad networks.

BitClave's solution enables companies big and small to participate in an open ecosystem. Our innovative *decentralized search* technology is market driven, meaning businesses can optimize marketing investment with real results, consumers are incentivized to participate, and anonymity and data privacy are in the hands of each individual party. As shown in Figure 2, this ecosystem creates a win-win situation for customers and businesses, while eliminating the need for advertising middlemen.

BitClave makes it possible for the first time to optimize the seller-consumer value chain. In the *BitClave Active Search Ecosystem* (BASE), market economics drive incentives for data sharing that properly balances the tradeoff between market efficiency and personal privacy. Data still has immense value, but consumers and businesses have the power of choosing whether or not to share it. By eliminating forced data sharing and wasted revenue from today's large advertising network solutions, everyone wins. BitClave's open BASE ecosystem ensures innovation will continue in the advertising market as technology continues to evolve.

Example Use Cases

The potential for disruptive applications built on our BASE platform are significant. To highlight the BASE architecture and potential benefits, we illustrate several example use cases as well as a detailed case study in the automotive sales retail space, with mixed online and offline components. Our choice of use cases is partially informed by the "cost-per-click" data corresponding to how much a business has to pay Google everytime a user clicks on their ad[5]. The most expensive keywords, including "lawyer", "insurance", and "degree", are in the range of $45-60 per click, regardless of who is clicking or whether they follow up with the business. Each example is further built around the main idea that personal information collection is crucial for high quality targeted offers. Since personal information can be contributed to BASE in various ways, including in the user registration process and as part of search requests, we particularly highlight the roles of anonymization, data protection, and customer consent.

Lawyers and Legal Advisors

Due to the unique and varied nature of legal cases, sharing personal data can be critical in finding the right professional for the job. With each individual case full of nuanced information, it's challenging for people to communicate all of the details and for a lawyer to have enough information to make informed decisions, especially in the early stages of a relationship. In situations like this, personal data can help legal professionals determine if they could be a good match for the potential client. BASE supports the ability for a user to post personal information and transaction history in a protected way, such that the user can later choose to share selected information with a potential legal professional. If particular user data would be useful to the legal professional, the user can choose to reveal it to them, without revealing it publicly. This

[5] E. Gabbert, "The 25 Most Expensive Keywords in AdWords – 2017 Edition!", July 2017, http://www.wordstream.com/blog/ws/2017/06/27/most-expensive-keywords

data may further allow the legal professional to target more desirable clients and personalize offers of service to them.

Educational Degree Programs

In the crowded marketplace of educational institutions promoting similar features and benefits, it can be difficult for a potential student to discover which school is the best fit. When the largest universities with significant advertising budgets can outbid smaller institutions for advertising space, these smaller schools lose opportunities to connect with students who might be a perfect match for their community. Students are missing out on information that can help them make the right decision, while institutions of higher learning are struggling to meet enrollment goals. Schools are turning to new technology to help find the right students who fit their academic and community profiles, and they are spending thousands of dollars on advertising with the hope of reaching interested students.

Suppose a student is about to graduate from high school, and they are searching for a program in Biology at a university near their home town. Using BASE, they can search for Biology degree programs, and information already stored privately in their BASE profile can guide potential university admissions coordinators to respond to their search with details of their highly relevant program, rather than finding the institutions that spend the most on advertising. Unlike third-party networks, BASE creates more relevant connections between the student and degree program based on the ability to selectively share the most relevant information for the search. The student can now choose to engage with personalized ads identified through BASE and earn CAT tokens to support further searches or even to pay program application fees, if supported by the school. More importantly, because the student has received the specifically targeted ad, they know that the school is interested in their application, building confidence in the match and motivating the beginning of a fruitful relationship.

Jobs Search

Similar to the use case of matching students seeking to further their education, BASE can be used as a job search platform. Job seekers can use the BASE decentralized search platform to search for employers, while employers can find potential employees with particular skill sets. Of particular value in the hypercompetitive technology job space, BASE can be used as a sort of “reverse job search”, where job seekers can anonymously post their job interests and core skill sets, and employers can target particular job seekers of interest to advertise custom-designed job positions tailored to fit the needs of the company and the unique skills of the employee. This is a sharp contrast to traditional job search boards where employers post generic “Software Engineer” job positions that lead to high turnover rates within the company.

Local Community Services

As an extension of the above job search usecase, BASE can be used for local community low cost peer-to-peer search for low cost services. For example: tutoring, babysitting, dog walking services offered by

teens or students within the local community. BASE can be used as an accessible, free platform where young people can advertise the services they offer or fulfill some requested services. In this use case the emphasis is not on high skill jobs, but on peer-to-peer local community errand-like tasks, that in addition to the value of executing the task itself also assist in building local community.

Asset Management

Planning for retirement is on the minds of many working professionals. However, personal finance records are highly private and many are not comfortable providing this information through unsecured channels. Without the personal information of the individual, it can be challenging for asset managers, financial planners, and loan officers to provide the most accurate information to their potential clients, leading to missed opportunities for both parties. An individual looking for a financial planner using BASE can search for firms who specialize in specific income ranges or investment strategies and make key personal financial metrics viewable only to those firms who meet the individual's criteria. A search for financial planning firms will return results from businesses that have identified the individual as an ideal client, and when the individual interacts with the offers and opts in to sharing their data through the secured BASE platform, the business can customize and personalize their service offers.

Automotive Sales

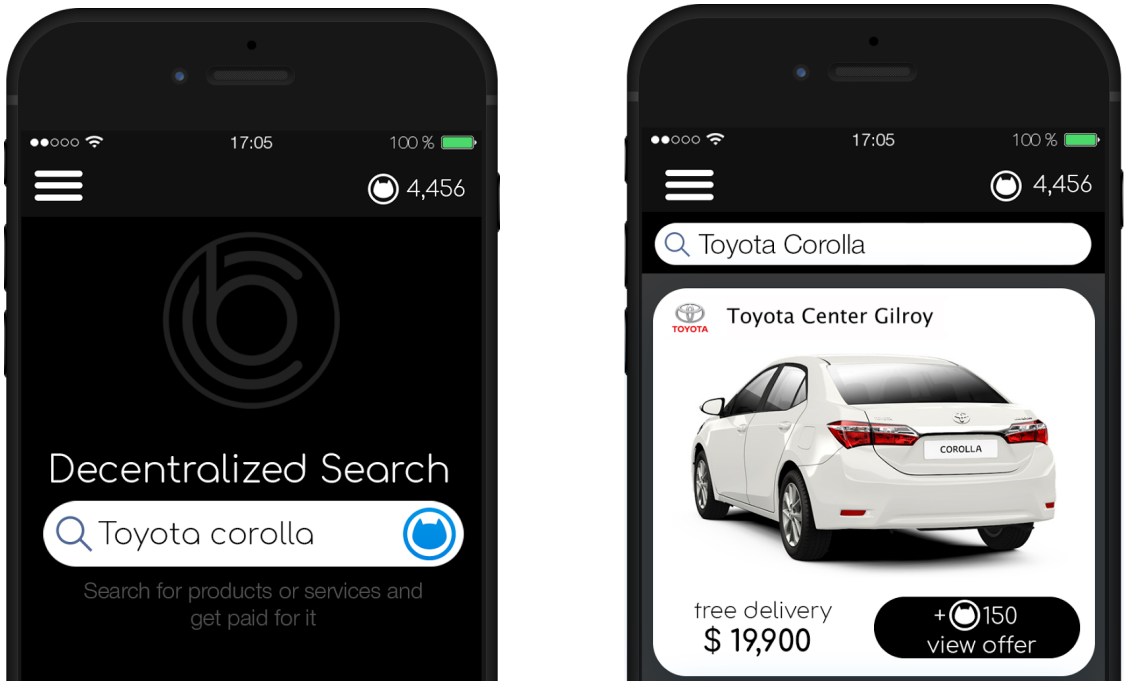
We'll describe the automotive sales use case in greater details as it presents several unique challenges that our BASE platform can address. As in many sectors, customer acquisition is a business-critical and costly sales component. In the car dealership industry, this factor is key to operating a successful 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 effective 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 a $100 prepaid gas card or six months of roadside assistance service to help close deals. Additionally, these “deal sweeteners” are provided to car dealerships themselves by the automotive-focused referral services as incentives to justify their high membership costs. In terms of sales and satisfied customers, the budget spent on acquiring leads is better spent on direct promotion offers to the customer. The BASE platform, facilitating direct customer-to-business engagement and innately vetting leads for quality, is precisely the solution for redirecting wasteful targeting expenses to enhanced customer relations.

In the BitClave Ecosystem, illustrated using the mobile app mockup in Figure 3, an automotive dealership will have the opportunity to display their promotions and advertisements directly to a potential buyer using precise, data-driven targeting. At the same time, the dealership will be guaranteed that their content is viewed by legitimate buyers, rather than random parties who are uninterested in the content or bots. The dealership will have the option to filter potential customers by a wide variety of factors, including examples such as owning a car for more than two years or having a child who recently reached the legal driving age.



(a) (b)

Figure 3: A mockup of the BitClave decentralized search application on a mobile device includes (a) a streamlined search interface and shows the user how many CAT tokens they have earned that are available to use in the BASE system. After searching for a product or service, the app presents (b) potential offers with CAT incentives for viewing the offer details.

One of the major benefits to the dealership of using the activity ledger in BASE to record interactions between the dealership and their customers is that relevant data about customer purchasing history and preferences are securely stored in the ledger. This data can provide valuable insight to the dealership marketing team, including when to resume advertising to a previous customer, when to offer service

discounts, or what types of accessories the customer is interested in. Data stored in the BASE ledger may further indicate a customer's "rating" that relates to the frequency of interacting with ads and the associated conversion rate. With access to these ratings, the dealership can assess the value of advertising to each customer, in order to optimize their advertising strategy and return on investment. For instance, if the customer rates highly on viewing ads and promotions but low on conversion after viewing them, the business may decline to further target the customer due to low chance of resulting in a purchase. Similarly, analyzing customer activity over time may allow a dealership to learn which promotions are successful, enabling them to improve services and promotions in a cost-effective manner and again maximizing return on investment. These examples demonstrate the value of the BASE platform over traditional advertising models, even for the complex and competitive world of auto sales.

Technical Solution 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), where every participant in the BASE system is incentivised by Consumer Activity Tokens (CAT).

The initial vision for the BASE and CAT is based on Ethereum technology—an open source, blockchain-based, distributed computing platform which utilizes smart contracts. These cryptographically secure smart contracts are stateful applications stored in the Ethereum blockchain, fully capable of enforcing performance. While Ethereum is the initial target, we may transition to a different blockchain technology if appropriate. See more details on the potential alternative blockchain technologies in the section below.

BitClave Active Search Ecosystem (BASE)

BASE relies on blockchain for storage and management of vast amounts of data related to customer activities in the search ecosystem. These activities are created by software endpoints operated by either the customers themselves or by the retailers they interact with. As such, various forms of software applications including retail websites and marketing dashboards can read to and write from the blockchain; for example these integrations could be used to build valuable audience matching knowledge based on customer preferences and shared demographic information, or to learn about the businesses that offer a particular product. As the BASE ecosystem is decentralized and open, anyone can create such software that interacts with customer and business data published to the blockchain. Instead of releasing and selling this data to monolithic advertising service providers, businesses and customers have control over the data they contribute to the blockchain as well as whether the data is shared publicly or protected cryptographically, with access further controlled by the user.

Of particular note, user-facing software has the capability to anonymize information contributed to the blockchain, creating what we refer to as the anonymous activity ledger. Activity anonymization is done in a way that allows only authorized parties to attribute multiple activities to the same customer. For all other parties, the data is not attributable to specific individuals (or linkable beyond certain lengths of times) while remaining valuable for statistical and data aggregation purposes. This gives the customer control over what data is allowed to be created, shared, and accessed, all managed and enforced through the use of blockchain and smart contracts.

As the anonymized activity ledger is the foundation of the BASE retail infrastructure, providing a decentralized capability for the crowdsourcing and sharing of data describing anonymized customer and

retailer activity, it facilitates a variety of analytics capabilities that leverage activity data from customers, stores, mobile apps, websites, and other sources across different retail domains. As previously mentioned, any party can contribute (potentially anonymized) data to the activity ledger, and any party can potentially get value from the data, depending on whether the contributor has encrypted or masked the data in any way. Similarly, the value of a given data asset (valued in CATs) can be owned by a customer, business, third party service provider, or some combination as specified by the smart contract whereas control over use and disclosure of personally identifiable data is retained by the user.

Users may contribute data to the activity ledger in many different ways. They can initiate a profile, including personal information such as demographics (e.g., age, income bracket, city/region of residence) as well as search preferences, interests, and any additional information they feel is relevant to their search. Furthermore, when a user posts such information, they can choose to post it in the clear (so it is truly public) or protected cryptographically, which may allow them to selectively reveal their personal information to some, but not all, retailers.

Additional sources of data include

- the history of the searches for goods and services through user-facing applications, as each search query is published to the blockchain,
- and actual business transactions between customers searching for products or services and providers of such products or services.

Again, the user can configure how information is revealed or protected within the search queries, for example by anonymizing their identity or applying cryptographic protections to the search terms or metadata fields.

In addition to explicit searches, users can indirectly contribute activity data related to visiting websites through the use of authorization buttons, similar to the “Login with Facebook” button that authorizes a third-party website to authenticate/authorize a user using their Facebook credentials. For example, a user browsing on their favorite retail website can create a record of this activity by clicking a “Record My Visit to BASE” button, hosted by the retail website, that posts their browsing activity to the activity ledger on their behalf. This type of activity sharing is still controlled by the customer, as clicking on the button represents a sort of “opt in” to sharing this activity to the blockchain. As such, this capability would rely on suitable authentication and authorization protocols, such as OAuth, to ensure that the retailer cannot post without the user’s consent.

Structure of BASE Activities

In order for activities posted to BASE to be useful to interested parties, activity entries posted to the ledger should adhere to a standard format. While the official definition of this format will be determined at a later time, at a minimum, each activity entry should include (1) an activity tag to identify the type of entry, (2) the unique identifier (e.g., hash of the user’s public key or a suitable anonymized substitute) of the user, (3) any descriptive details required for the activity type, and (4) a timestamp. An initial list of supported activity types and corresponding metadata entries will be provided, but the BASE community will be free to define and

introduce new activity types as the ecosystem grows.

Examples of initial activity types include:

REQUEST
Customer-facing software can publish a shopping preference, item of interest, or personal preference reflecting an intent to purchase goods or services. An example of metadata supporting a REQUEST is the timeframe for the purchase, which would imply an expiration data/time of the search.

OFFER
Retailer-facing software can publish a short-term offer for discounted items or services, either publicly or targeting specific users based on REQUEST activities. OFFERs can include similar metadata as REQUESTs, for example to represent a limited-time offer.

VIEW
Customer and retailer facing software interact, where the customer facing side publishes a unique confirmation (Proof-of-View) that the customer viewed the offer and the business side verifies that the confirmation corresponds to the correct OFFER. A confirmed VIEW event will trigger CAT reward from retailer to customer for viewing the OFFER.

BUY
Customer software can publish an activity to indicate the user has executed a purchase from a particular retailer, possibly including descriptions of the item(s) purchased, price, seller, etc., any of which can be cryptographically protected for selective access.

SELL
A retailer's point-of-sale software can publish an activity (possibly corresponding to a user's BUY activity) to indicate a sale has been made, possibly including similar details as a BUY activity, again noting that any or all data fields could be cryptographically protected for selective access.

Note that certain activities (e.g., BUY/SELL), although implying a counterpart activity, may or may not appear in pairs, as either party can choose not to publish their respective activity to the ledger. This basic format for an activity is shown in the following table, including a description of each field in the right column.

Activity:	<act_tag>	Tag used to reference this activity from elsewhere
Orginator:	<cust_tag>	Anonymized tag used to reference activity originator
Activity	<activity_type>	Activity type, e.g., REQUEST, BUY, SELL, 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)

Figure 4: Activities posted to the ledger as blockchain entries include various pieces of information including an activity reference, a (potentially anonymized) tag identifying the creator of the activity, and a variety of details about the activity.

To illustrate the activity data format, we illustrate potential activity blocks that would be created in an online search for a new car, where <angle brackets> are used to indicate fields that may be encrypted or otherwise protected.

Activity 4E773C91	
Organizator:	<A>
Activity:	REQUEST
Activity details:	Toyota Corolla
Timestamp:	1496318700 UTC

Activity 36EA9801	
Organizator:	<A>
Activity:	VIEW
Activity details:	PoV code: 0×236831156
Timestamp:	1496318885 UTC

Activity 4E773C91	
Organizator:	<A>
Activity:	BUY
Activity details:	QR code from dealership
Timestamp:	1496318943 UTC

Figure 5: Examples of activity entries in the leger include a search request for a new car, a potential customer viewing a targeted ad, and a customer purchase. Each activity includes (potentially anonymized or otherwise protected) entries about the interaction.

The relevant activities themselves (indicating the search, advertisement offer, visit to dealership website, and purchase) already provide useful customer data to the auto dealership and its current and future customers. In particular, even without knowing the customer's true identity or specific details of their search or web visit (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 the relative number of purchases to ad offers (a proxy for the ad conversion rate or customer sentiment about the dealership).

Other entries and data in the activity block can be encrypted or anonymized to protect identifying

information or other sensitive data

This example of direct marketing between car dealerships and customers interested in buying vehicles demonstrates the B2C interaction that BASE and the anonymous activity ledger enable. We further elaborate on this example to demonstrate how this interaction would work in an end-to-end example.

Example: Direct-to-Consumer Auto Marketing

Direct marketing can leverage explicit REQUEST activities created by potential customers, as illustrated below. Retailers can analyze numerous REQUESTs 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 REQUEST, 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.

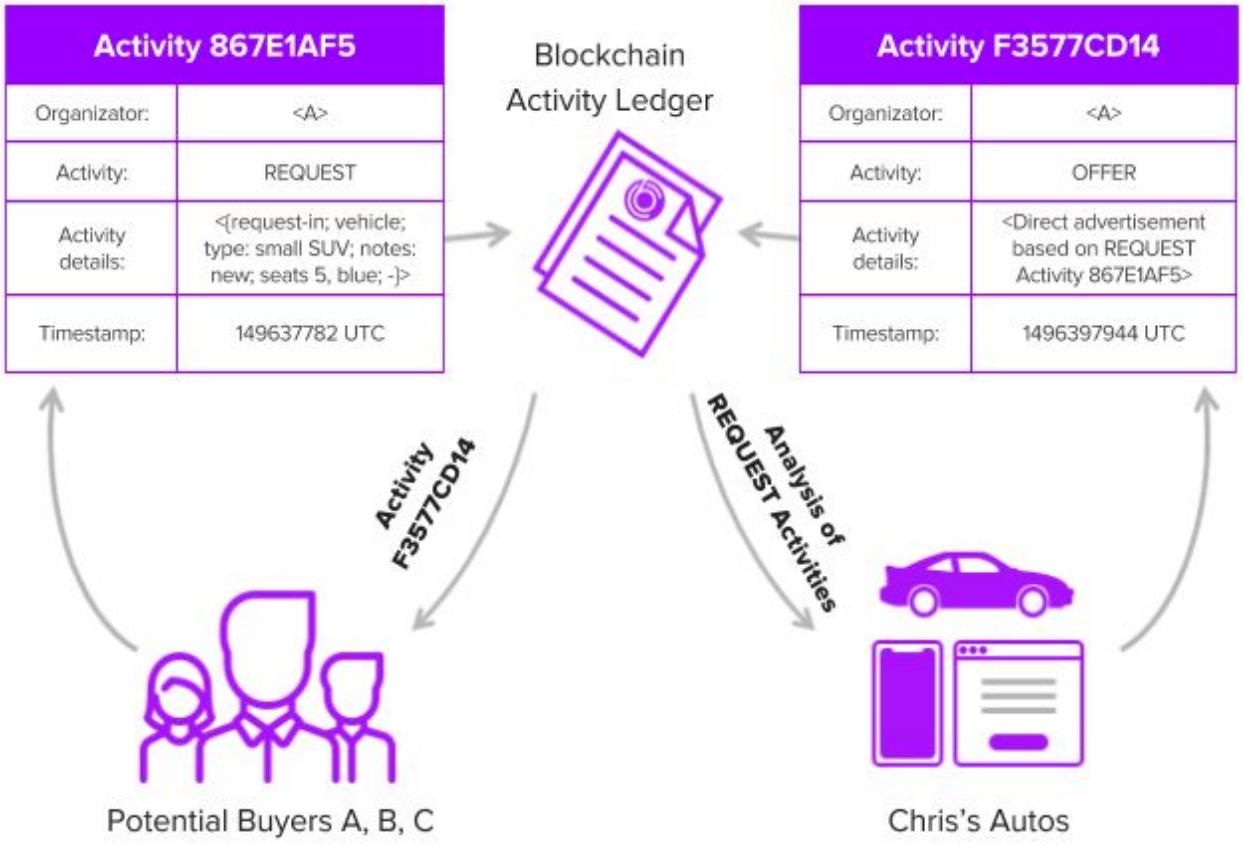


Figure 6: We illustrate the flow of information between potential customers and a car dealership through the activity ledger, including REQUEST activities representing customer searches and OFFER activities representing targeted ads from the dealership.

Customer and Retailer Anonymity In the Activity Ledger

As mentioned above, certain aspects of customer and retailer information stored in the BASE activity ledger can be anonymized to protect customers' identities, information they consider sensitive, and their overall search history. We first describe the possibilities, roles, and challenges associated with anonymous activities, and further technical details will be provided in a later section.

At a high level, anonymity can be achieved by allowing a single user to post to the BASE activity ledger using a variety of unrelated pseudonyms, or alternate identities. We note that the use of multiple identities is already supported in many blockchain platforms, as any customer can create an arbitrary number of accounts, wallets, or public key identifiers; this is already common in cryptocurrency platforms like Bitcoin. There are several reasons, beyond privacy, that a user may want to do this. For example, suppose that a user uses BASE while shopping for business needs and also for personal needs. If both of these tasks are performed using the same identity, as is typically done today through monolithic ad networks, both of these roles are combined into a single "customer profile", so the user will be shown ads that relate to both their business and personal lives. If however, a user could create two separate personas, based on different pseudonymous identities, the search activities could be effectively isolated from each other, allowing the user to separate the ads they see based on their current role. While the different pseudonyms approach solves customer concerns with regards to anonymization, it introduces a challenge for businesses as now they need to have a way to know that two different pseudonyms asking for a service actually belong to the same person, to prevent paying out a reward twice. Solution to this problem is described later in the document.

In a more general sense, user-facing software can support the use of multiple pseudonyms for a user's search activities, either in support of multiple personas as above, or to truly anonymize the user's search with a different pseudonym for each activity contributed to the ledger. Even in this case, BASE supports the ability to later allow the user to selectively reveal information about these anonymous posts. Specifically, metadata can be included in the activity's fields that can later be used to reveal the true identity of the user or to reveal links between different pseudonyms (even without exposing the user's true identity), noting that both of these can be allowed selectively to only a specific list of authorized parties. More technical details about how these anonymization and selective linking capabilities are provided in a later section. The following example highlights a few key details of identification and tracking, both of which BASE aims to prevent by default.

Example: Linking a sequence of activities for multiple retailers

We provide an example scenario to highlight the benefits that can be attained by de-anonymizing or linking anonymized activities in the ledger. Suppose a person is involved in a serious car accident, and as a result, they need to find a lawyer, a new car insurance provider, a chiropractor, and an auto repair garage. The user turns to BASE to search for relevant service providers. For each of their searches, the user publishes a REQUEST activity to the ledger, each using a different pseudonym instead of their true identity. However, many of these providers may offer better rates for their respective services if they know about the other

services the customer is seeking. For example, subscribing to a car insurance provider may lead to discounted auto repair. More importantly, if a service provider can link together the many activities to understand the unique situation that the user is faced with (in this case, trying to quickly recover from the car accident), they can be more confident that an OFFER they make to the user will convert into a sale. Because of this confidence in a strong lead and expected sale, the provider may even choose to make a stronger OFFER to the user based on the shared linking among the activities.

Consumer Activity Token (CAT)

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 BASE ecosystem among the participating parties. CAT tokens will be used to facilitate rewards within the system for a variety of services available in BASE. The CAT-based market puts power into the hands of businesses 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 software capabilities such as data analytics that operate over the data contributed to the blockchain.

BASE solves a real problem for businesses and consumers. Businesses and customers are the main participants as they get most benefit in BASE. Other than business and consumers, in BASE there is a place for many other participants in roles of service providers, like Search Services, Ranking Services, Analytic Services that will benefit from BASE economics. The following section describes in more details the incentive each participant gets from being an active part of BASE ecosystem

Tokens as Incentive for Participation

As the basis for supporting interactions in the BASE ecosystem, the data contributed to the activity ledger is of key importance. As such, any activity contributed to the ledger has potential value to BASE as a retail marketplace. Whether user-contributed REQUEST data leads to direct CAT rewards, however, depends on whether a retailer chooses to respond with an OFFER to that user, which further depends on other REQUESTs that have been posted by other users' searches. Because of the open nature of BASE, there is a natural notion of competition for these CAT rewards. For example, suppose two users X and Y post REQUESTs for the same product, but Y provides more supporting personal information in their REQUEST. Since more information likely implies stronger seller confidence that an OFFER will convert into a sale, a

seller may prefer to send an OFFER to Y rather than X, or they may send a more valuable OFFER to Y than to X. In this case, while neither shopper is directly paid for their data, Y has made a conscious decision to reveal more information to make their search more attractive to retailers and therefore more likely to succeed. In this way, BASE more directly represents a free market economy, as the relative value of contributing different types of activity data to the ledger are determined indirectly by the market economics of the system.

Retail Analytics Providers

The unique nature of the BASE market creates opportunities for additional roles beyond buyer and seller. Since the REQUEST and OFFER activities likely rely on some understanding of the various customers and retailers, an entity can participate in BASE in the role of an *analytics provider*. In this role, an entity can create and sell custom analytics capabilities to various users in BASE, effectively extending the market to include supporting services as well as commercial goods and services. This makes BASE a natural supplement to any eCommerce company's marketing or customer relationship technology stack. As such, any eCommerce merchant 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.

Technical Solution Details

Main BASE components

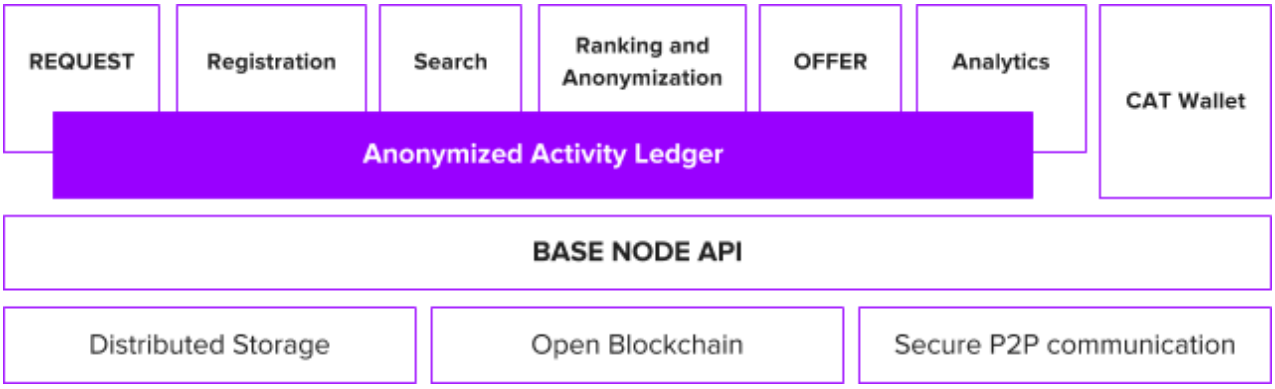


Figure 7: The various components of BASE that comprise the activity ledger are built on the foundations of blockchain, off-chain storage, and secure communication capabilities among relevant parties. The BASE API provides a layer of abstraction to ease development efforts and support a level of flexibility regarding specific blockchain implementations.

Registration subsystem

Interaction with BASE starts with the registration process. Every participant in BASE will have to go through this process. Since BASE is a decentralized system, we need to have schemes to prevent malicious users from taking advantage of the system. The basic scenarios we want to prevent are for users to report fake personal information to businesses to get better OFFERs or for users to open multiple accounts and receive rewards for searches multiple times. These are just a few rogue schemes to emphasize the challenge.

The Registration Service is responsible for verifying customer/business information wherever possible. Registration Service is a registered entity in BASE by itself. Registration Service will be identified by its public key, so every interested participant will be able to verify the authenticity of the information signed by the Registration Service, but only Registration Service will be able to create such a signature. It is up to a user to decide which Registration Service to use and what information to disclose for verification. BitClave will implement a Registration Service but other interested parties could implement an alternative version if desired.

Once a user registers within BASE, the Registration Service, after the user's consent, will verify the provided personal information (or parts of personal information) that the selected Registration Service is able to verify. The verified personal information will be signed by Registration Service and will have "higher" value when is used by businesses to provide OFFERs. For example if the salary information and the current cars of the users are verified, it will give more confidence to a car dealer when generating a personalized offer. Users

can always opt to verify personal information later, once more comfort with the system is established. After registration is complete, the personal information of the user will be stored in blockchain in an encrypted way. No one will be able to understand it, but the user will be able to provide a key to the parties based on choice, so these parties can decrypt the personal information and also check if the information is signed and verified by one of the Registration Services.

REQUEST Subsystem

When customers interact with BASE, they mainly interact with the REQUEST subsystem. Here, customers can submit searches as REQUEST activities, receive a list of OFFERs, interact with OFFERs to receive rewards for viewing, and complete sales transactions.

The REQUEST subsystem represents customer interests. In decentralized systems we have multiple entities for search and multiple businesses responding to customer REQUESTs. These entities pursue their interests or could be just malicious entities. The main role of REQUEST

subsystem is to protect customer interest and maximize BASE value to customer. Some of the most important roles of REQUEST subsystem include:

- Filter out spam or OFFERs that do not satisfy customer REQUEST. This could happen by mistake or intentionally when posted by some malicious sender.
- Filter out not-trustworthy businesses, for example business with low ranking or businesses with not confirmed registration status.
- Prioritize search results from multiple search engines based on criteria customer selects. While this prioritization could be implemented in customer UI layer, implementation in contract layer would be visible to other entities and will further improve business ability to provide the best matching offer.
- Collect relevant personal information as part of REQUEST process. For example, while looking for car insurance, the system might ask for a more detailed questions like current house insurance, previous car insurance or life insurance. While these questions would be of a concern to answer in initial registration phase, a customer will be more comfortable to provide these in context of insurance search query. Of course, customer can decide not to provide this information and he would still receive offers but these might be not as good as offers based on a more detailed personal information. Once additional personal information will be provided as part of the search it will be securely stored with customer account on blockchain in an encrypted way and later could be used, with customer consent, in other REQUESTs.
- Recommend customer what private information to reveal to get a better OFFER. Usually, OFFER will include different reward based on customer personal information (that's the the whole point of targeted/personalized offer). When REQUEST subsystem is receiving an offer, it can identify what personal information would result in a better reward for the customer and would recommend to customer to expose that information to the offer. Customer then will make decision to expose or

not, based on additional reward, level of trust to the proposing business and other criteria.

- Interact with R&A service to assist customer in selection best anonymization approach for his REQUESTs. We discuss below various approaches for anonymization, so here Request subsystem, representing customer interest, would recommend the most suitable approach for a specific transaction

OFFER Subsystem

When businesses interacts with BASE, they mainly interact with the OFFER subsystem. Business can submit OFFERS to BASE, define OFFER structure based on individual customer information, run data analytics to understand what OFFERs are working and other related activities.

The OFFER subsystem represents business interests and has many similar features to the REQUEST system above, only on the business-facing side rather than the customer-facing side.

The most important roles of the OFFER subsystem include:

Identify scammers or not trustworthy customers, as in the REQUEST subsystem but now focusing on protecting business interests.

Prepare targeted OFFERs based on specific customer personal information, customer ranking and customer search request. This is very similar to the roles of REQUEST subsystem but in the “reverse” direction and with focus on protecting business interests.

Verify “proof-of-view” reports before sending to customer reward for viewing the offer. Click fraud is major issue with online advertisement. While addressing customer privacy concerns by anonymization schemes, we need to address key business concern of how BASE would prevent click frauds by scripts or malicious users. Quite a few solutions are available on market today, and BitClave is going to pick a combination of proprietary and off-the-shelf solutions for protection of business.

Search Service

Search Service is an independent entity that is matching REQUESTs with OFFERs. Search Service incentive is to maximize the number of transactions in BASE. Search Service could be optionally incentivized by CATs for successful transaction. A variety of different Search Services could be employed in BASE, with some trying to optimize the customer experience and others trying to maximize business value. We do not want to impose any strict constraints on the Search Service, rather allowing for competition in the ecosystem, while

customer and business interests will be protected by REQUEST and OFFER subsystems respectively.

Search Services can be very specialized, focusing on local services like plumbers, babysitters, school tutors, cars, lawyers, financial advisors and more. BASE is designed to support multiple implementations for any service in the system.

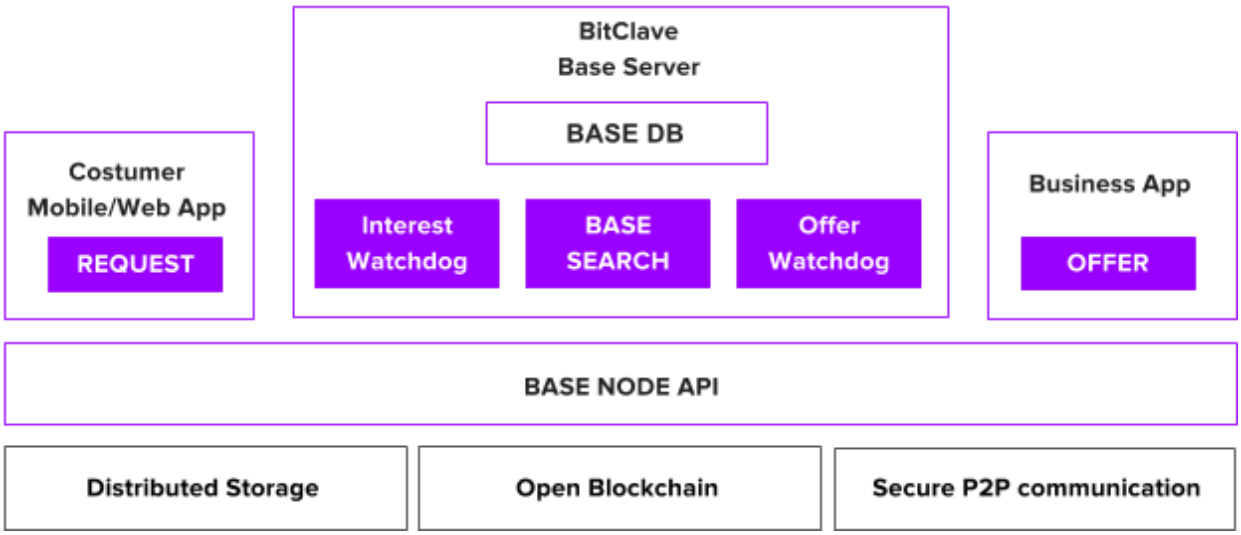


Figure 8: The BASE architecture shows how the various services play interactive roles between customers, businesses, and the blockchain-based ledger.

As mentioned above, the role of the Search Service in BASE is to provide a “recommendation” to REQUEST or OFFER smart contracts on potential matches. The final decision to make a

business transaction is made by the user and is facilitated by smart contracts on-chain. The role of the Search Service can be compared to the role of a realtor in the real-estate business. The realtor will bring together a potential buyer and seller, but the final decision on business transaction is made by the individuals.

Here are some details about BASE Search Service Implementation. To implement BASE, BitClave assumes two roles:

One role is to implement an open, decentralized platform that enables direct customer-to-business interaction with no need for intermediaries as in third-party advertising networks.

The other is to implement all applications and services required to bring this platform to users. These include the Search Engine, Clients, Business apps, and more.

Remember, BitClave's goal is to build a platform with no intermediaries. It means BitClave is committed to define an open platform, hence its implementation will use only information that is available to all. *This transparency guarantees BitClave itself is not playing the same role as the middlemen in advertising.* In addition, BitClave will provide its implementations for Search and other components as open source software.

BitClave, in the first capacity, will store anonymized information about customers, businesses, offered product/and services in a combination of on-chain storage and off-chain open, decentralized storage available to all.

In its second role, BitClave will use off-chain entities to enable efficient search. These entities will include external servers that will retrieve information from open storage (in a read-only way) and will populate BitClave's databases that are optimized for search. When new search requests enter the blockchain, BASE will use its database to find the matching offers and will communicate these offers to the smart contracts on blockchain. The final decision to make the transaction is done by the user and is facilitated by smart contracts. Recall from above, the Search Service is just providing recommendations.

We note that nothing prevents any other interested party to implement a more efficient blockchain-based Search Service. Thanks to its open-source nature, BASE will only benefit from alternative and better implementations of Search Services, and with continued engagement from BitClave's users and partners, along with advances in blockchain technology, the recommendation engine will improve and enhance the performance of the entire ecosystem

Ranking & Anonymization Services

Ranking in a distributed and anonymized system is a challenging subject. On one side, customers may want to be anonymous, so they may use different pseudonyms for different activities in BASE. On the other side, businesses want to provide OFFERs to customers whose

interests are more relevant, but in order to build a ranking, one needs to correlate activities (including searches, purchases, and profile details) across multiple different customer pseudonyms. To discuss our approach, we use a variety of terminology related to identity, anonymity, pseudonyms, and linkability that are consistent with the Common Criteria ISO/IEC 15408 standard for Information Technology Security Evaluation

[6].

At a high level, to maintain openness in the BASE ecosystem, we plan to create various options for users to select, so they have control over their own tradeoffs between anonymity and search value. We next describe how we intend to address the conflict between customer desires for anonymity and businesses need for linkability.

Ranking by Customer ID

At one end of the tradeoff, a customer can sacrifice anonymity completely by using their primary blockchain wallet identity in all of their BASE transactions. In this simplest mode, all of the customer's information (whether public or protected) is linked to their true identity in the ledger, so any other party can perform a variety of analytics of the customer's search and purchasing history, for example computing the ratio of purchases to offers (i.e., their conversion rate). The disadvantage for customers in this mode is that all historical transaction activities can be linked together. While some customers may choose this approach that maximizes search value (while still protecting individual transaction details, of course), others would be uncomfortable releasing this much information about their transaction history.

Even with complete linkability, we want to protect the customer data involved in individual transactions and enable selectively revealing information to businesses. To realize this

ability, we could include a list of encrypted customer data, along with the search query, where each list item is encrypted using a symmetric key that nobody else knows. This is an example of what is called a cryptographic commitment, because it doesn't reveal any of the information, but binds each piece of information to the search. For example, this list could contain values like

$$E_{k1}(info_1), E_{k2}(info_2), \ldots, E_{kn}(info_n),$$

where E_k denotes encryption with a symmetric key k and each piece of information $info_i$ is encrypted using a different key k_i. If the customer later wants to reveal a specific piece of information $info_i$ to a retailer, such as his purchasing history or some demographic details, the corresponding key k_i can be securely communicated to the business, allowing them to decrypt the relevant data. As an example of how this would be transmitted, the customer could, for example, send the encrypted message $E_{PKj}(k_i)$ to business j, where E_{PKj} denotes asymmetric encryption using the business's public key PK_j. This action (referred to as opening the commitment) allows the retailer to access the customer's private information without changing any past commitment, since the blockchain prevents modifying past data.

[6] 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.pd

Ranking by Pseudonyms Initiated by the Customer

In a step toward stronger anonymity, the customer can choose to use pseudonyms for different activities in

BASE, so the activities cannot be linked together. While this protects the customer's search history, it hides useful information from businesses. In some cases, the customer may want to reveal certain links to a business, for example to facilitate many of the use cases described previously. This could be useful to prove that a customer purchased a new car and now is looking for insurance or to demonstrate repeat business, such as buying running shoes every few months. Ideally, the customer can expose certain links to selected businesses without (i) revealing ALL transaction history or (ii) revealing links to undesired businesses. Whether a customer exposes links will also depend on whether a business will actually provide added value to the customer for the information, as the businesses are not paying for the data directly, but that is a different concern.

To understand how we could implement this selective linkability feature in BASE, recall that the strictest use of pseudonyms would mean that every activity posted in the ledger would appear to come from a unique person, meaning true customer identity is perfectly obscured. In a slightly more practical approach, suppose a customer uses different pseudonyms for different search activities, for example using one pseudonym ID_{shoes} to search for new running shoes every few months. However, now suppose this customer wants to reveal some information from their public profile, which requires linking the pseudonym ID_{shoes} with the customer's real identity ID_{real} corresponding to the profile. There are many ways to do this, starting with the previous example where pieces of information can be encrypted and committed to the search. In particular, when searching using pseudonym ID_{shoes}, the customer can include an encrypted tag $E_k(sig_{SKreal}(k))$, which is an encrypted signature using the secret key SK_{real} corresponding to the true identity ID_{real}. This encrypted tag is meaningless without the key k, as the encrypted signature can be neither accessed nor validated without it. As in the previous case, the customer can securely reveal the key k to a selected business, which then allows the business to unlock the signature $sig_{SKreal}(k)$ and verify that it was signed with the correct secret key to prove the link between the pseudonym and real identity. Similarly, if customer wants to link together multiple pseudonyms (for example, if the customer did each search for shoes using a different pseudonym), a list of transactions and the corresponding keys can be shared to link them together, all without anyone else knowing this linking exists. Moreover, the linking could be done entirely among pseudonyms, without linking to the customer's true identity, if all that is needed is a proof that the searches were all made by the same customer.

However, with this type of exchange using pseudonyms instead of true identities, it's probably the case that an identity is more sensitive than other types of information, so we may want to provide even stronger guarantees. In fact, using an encrypted signature as above has a potential weakness that it is not bound to the pseudonym, just the real identity. Instead of committing the identity using symmetric encryption as we may do with other customer information, we can build a stronger cryptographic commitment that binds to both the pseudonym and the real identity in a verified way. Instead, we can construct a signature pair that uses both asymmetric private/secret keys SK_{shoes} and SK_{real} to prove the customer holds both identities. One possible way to do this would be to include the signature pair

$$S = [sig_{SKshoes}(k), sig_{SKreal}(k)]$$

inside the search when using the pseudonym ID_{shoes}, using a similar random value k as the input to the signature function for each secret key. When the customer later wants to prove to another party that he

controls both ID_{shoes} and ID_{real}, he can secretly share the value k corresponding to that specific search, and the other party can validate both signatures in S using customer's two public keys PK_{shoes} and PK_{real}.

Third-Party Ranking & Anonymization Service

Another approach to balance the conflict between ranking and anonymization is to leverage an additional service provider in the ecosystem. This Ranking & Anonymization (R&A) Service effectively combines the benefits of the above approaches and facilitates privacy- and anonymity-preserving transactions between customers and businesses. Using the R&A Service, a customer will post an encrypted transaction to the R&A Service, which will post the transaction on behalf of the customer, while making a private record of the customer identity. R&A Service will see all transactions from the customer and hence will be able to compute the true global ranking for the customer. R&A Service will post transactions using new pseudonyms each time and will attach the true customer ranking as part of the transactions. The specific implementation of the R&A Service is a combination of the above techniques, though with the assistance of a third-party service.

From the business point of view, when a transaction goes through an R&A Service, it is more trustworthy. The incentive for customers to use this mode is that it will provide higher confidence for businesses in comparison to working with anonymous customers. Customers can decide which R&A Service to use, if any. The incentive for R&A service would be to provide "useful" ranking capabilities, and it could charge CAT fees for its services.

To summarize, customers and businesses have many alternatives in controlling their private information and their respective activity histories. As such, they will decide what works best for them. Since BASE is an open and competitive marketplace, it will eventually reach an equilibrium point, where the level of anonymization, trust, and reward is optimized for the community.

Activity Analytics

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. The Analytics subsystem is tightly related to R&A subsystem. It needs to interact with customers and businesses through the ledger to correlate transactions, but its goal is to provide a more global view to interested parties so these could optimize their strategies.

Specific examples include:

- 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 suitable key management, encrypted search, or other techniques.
- Analysis of customer profiles, personalized OFFERs and BUY / no BUY activities would allow businesses to develop a winning strategies with regards to rewards to be offered to a certain

customers.

- In addition to activity analytics for the purpose of opportunity identification and prediction, parties can use the data from the activity ledger to verify claims (analogous to forensic evidence), for example to satisfy the conditions of a smart contract made with another party in the ecosystem.

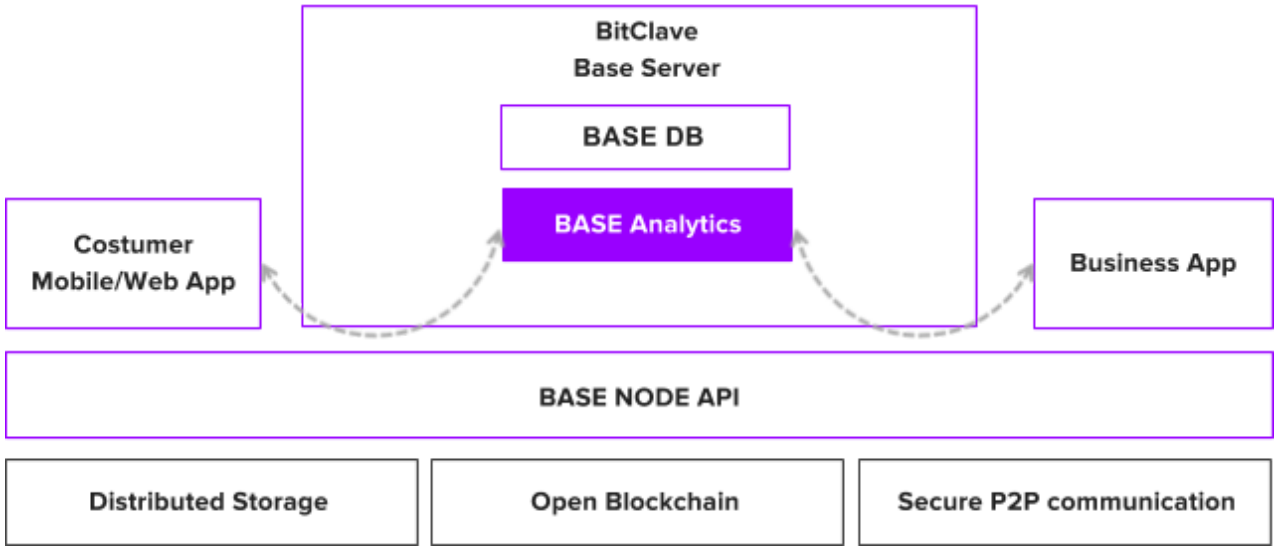


Figure 9: Analytics play an important role in BASE, providing insight to both customers and businesses in regard to histories of their respective activities in the marketplace.

The capabilities of the Analytics subsystem vary depending on the level of anonymization that customers and businesses use. To illustrate the variations, we provide a few representative examples of analytic strength as a function of anonymity level.

Case 1 (anonymity)

If a customer posts all of their searches using unique pseudonyms, corresponding to the strongest level of anonymity, it is impossible to compute any sort of search history, as each identity is used only once. In this case, the only way for a business to learn anything about the customer's search or purchasing history is to ask them to reveal more information, potentially relying on a smart contract that provides some added value to the customer.

Case 2 (linkability)

If a customer is willing to reveal links between their relevant past purchases but not willing to reveal their

identity or personal profile information, the analytics provider will be able to match the customer's purchase history to a particular predictive model that will suggest what other goods and services the customer may be interested in. For example, if the customer has linked activities for car repair services and personal injury lawyer services, the analytics provider may suggest promotions for car insurance or medical services, even without knowing the customer or any of their demographic information.

Case 3 (personal profiling)

If in addition to linkability, the customer is willing to reveal some amount of personal information from their profile, the analytics service can further improve the quality or value of the promotions suggested for the customer, providing stronger matches between the customer and potential service providers or better discounts in the promotions.

Based on the inherent value of analytics in marketing platforms, BitClave is planning to integrate with open source or commercial analytics platforms. The fact that BitClave maintains the read-only snapshot of the activity ledger significantly eases the integration with available solutions. This is a similar benefit of external snapshot as we see with BitClave Search approach. We note however, that the analytics subsystem is one of the advanced services envisioned for BASE, so it will be provided by BitClave at a later stage of development. As BASE is an open platform, other vendors could implement alternative competing Analytics services.

BASE Scalability and BASE NODE API

The vision for BASE is a fully decentralized, blockchain-based search platform where users and businesses can connect directly. This means utilizing enormous amounts of data, from both users and businesses. The pace of innovation in the blockchain domain is extremely high. While current leading blockchains like Bitcoin and Ethereum recognize scalability challenges and work on solutions for their blockchains, new platforms come to life with theoretically improved solutions - EOS[7], NEO[8], QTUM[9] are just few platforms to offer improved transaction speed. Innovation happens in many domains, not only scalability - improved anonymization like in ZCASH[10] and

MONERO[11], a more secure contract language like in QTUM, distributed storage systems like Filecoin[12] and SiaCoin[13], side channel solutions like Raiden Networks[14] or recent Plasma[15] announcement. To deal with

[7] https://eos.io/ - The Most Powerful Infrastructure for Decentralized Applications
[8] https://neo.org - A Distributed Smart Economy Network
[9] https://qtum.org/en/ - The Blockchain Made Ready for Business
[10] https://z.cash/ - Zcash is the first open, permissionless cryptocurrency that can fully protect the privacy of transactions using zero-knowledge cryptography
[11] https://getmonero.org/ - Monero is a secure, private, untraceable currency,
[12] https://ipfs.io/ - A peer-to-peer hypermedia protocol to make the web faster, safer, and more open
[13] http://sia.tech/ - Sia splits apart, encrypts, and distributes your files across a decentralized network
[14] http://raiden.network/ - High speed asset transfers for Ethereum
[15] http://plasma.io/ - Plasma: Scalable Autonomous Smart Contracts

such a high innovation pace and to be able to leverage the new solutions that become available, BitClave is introducing a BASE API layer that will abstract the underlying infrastructure services for distributed computing, communication and storage.

BitClave's main focus is to develop the BASE platform and the applications and services to bring the platform to users. This is where BitClave brings value. BitClave is going to ride the innovation wave and leverage new technologies as they become available or mature. BASE NODE API will help make this ride a lot smoother.

Ethereum Blockchain

BitClave will use Ethereum as the platform for initial release. Ethereum is a proven blockchain that provides the services required for BASE. With a strong roadmap, Ethereum's capability and functionality are improving continuously. Metropolis[16] with improved anonymity by zkSNARKS[17] and Serenity[18] with "Proof of Work" and "Proof of Stake" in near feature and Plasma in a more far future are just few examples to show Ethereum is a very appealing platform.

To illustrate the value each of these Ethereum improvements will bring to BASE, we provide the following use case of BitClave Search using Ethereum blockchain without any optimizations, followed by how each complementary technique would provide added value.

As a starting point, let's assume that BASE DB is already populated with OFFERs. In step#1, a customer submits search requests that are written to the blockchain. BitClave Search will detect that a new request was submitted (step#2). It will then perform the search within BASE DB to find the matching offer (step#3) and will write the proposed match to blockchain for OFFER contract to consider the proposal. The OFFER will read the new proposal (step#4), perform internal verification of the recommendation to make sure

Search recommendation meets the search requirements, and start communication with the original REQUEST contract (step#5). As part of step #5, OFFER will propose to REQUEST, and REQUEST in turn will verify that the offer matches the rules (reminder, none of REQUEST / OFFER / SEARCH are trusting each other). REQUEST will present the offer to user, who may decide to view or not to view the offer, and if the offer is viewed the proof-of-view has to be submitted back to OFFER to confirm the reward. For simplicity of the diagram, we combine all these steps in communication between REQUEST and OFFER under one bidirectional arrow for step#5.

[16] V. Buterin, "Ethereum R&D Roundup: Valentine's Day Edition", Feb 2017, https://blog.ethereum.org/2017/02/14/ethereum-rnd-roundup-valentines-day-edition
[17] C. Reitwiessner, "zkSNARKs in a nutshell", Dec 2016, https://blog.ethereum.org/2016/12/05/zksnarks-in-a-nutshell
[18] V. Buterin, "Understanding Serenity, Part I: Abstraction", Dec 2016, https://blog.ethereum.org/2015/12/24/understanding-serenity-part-i-abstraction

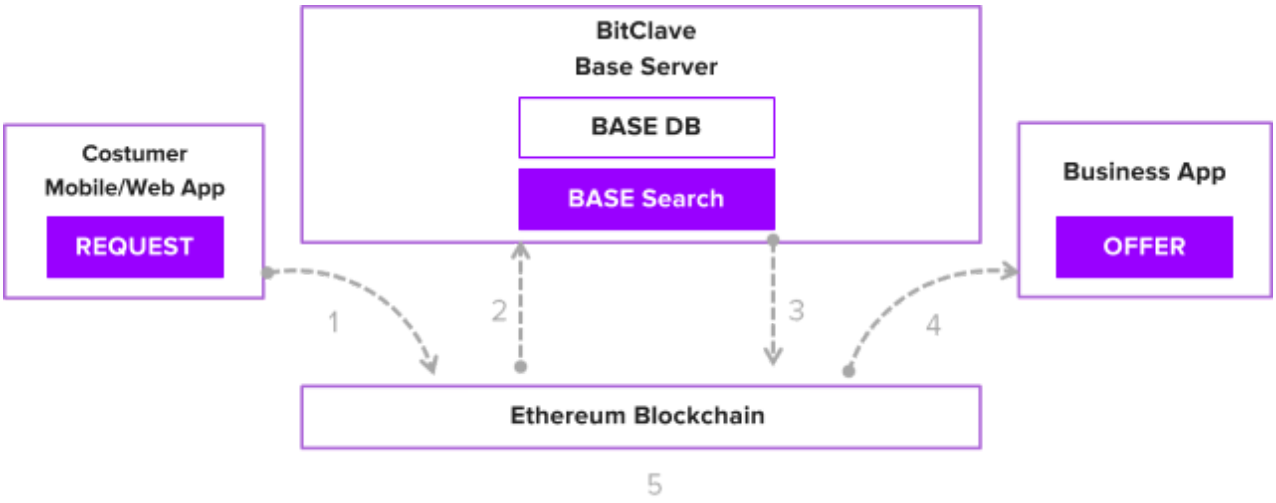


Figure 10: The flow of activities for a basis search activity is illustrated using Ethereum.

Storage Scalability

Ethereum provides a facility for decentralized storage. Unfortunately, the solution offered today by Ethereum is quite expensive. To store information on that blockchain, one needs to pay 20000 GAS just for a single instruction to store 32 bytes of data, which is about $0.02 when using average 4gwei for GAS price. When scaled by the number of transactions expected to go through BASE platform, the GAS fees alone reach millions of dollars.

Bitclave is looking for a better solution where it can significantly reduce the fees and gain performance. Multiple solutions are available today and BitClave is researching various technologies. IPFS[19]/Filecoin[20], Storj[21], and SiaCoin[22] are few technologies that the team is currently evaluating.

[19] https://ipfs.io/ - A peer-to-peer hypermedia protocol to make the web faster, safer, and more open
[20] https://filecoin.io/ - Filecoin: A Decentralized Storage Network
[21] https://storj.io/ - Blockchain-based, end-to-end encrypted, distributed object storage, where only you have access to your data
[22] http://sia.tech/ - Your decentralized private cloud

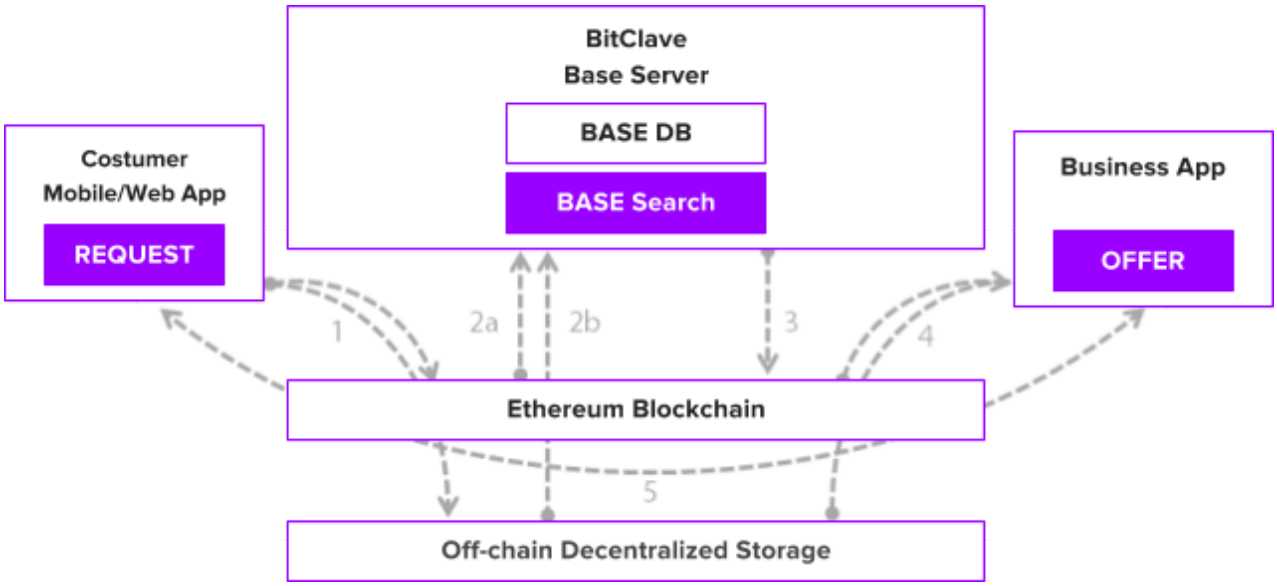


Figure 11: Using off-chain decentralized storage along with Ethereum will provided the added benefit of reducing the size of data published to Ethereum, thereby reducing GAS fees in exchange for communication with the public storage system.

To take advantage of "off-chain decentralized storage", will do the following modifications: when REQUEST writes to the blockchain, now only a single pointer will be written to the blockchain, while the rest of the data will be written to public external storage. Consequently, BASE search will have to follow pointers from the blockchain to access full REQUEST details from external storage. OFFERs will also follow the similar scheme.

Transaction Speed

Transaction speed on Ethereum is on the order of tens per second (see the recent CoinTelegraph announcement[23] for more accurate numbers). With more and more DAPPs to be deployed on Ethereum in the near future and with a large amount of transactions to happen on BASE, transaction speed might

[23] W. Suberg, "Ethereum Breaks Blockchain Transaction Record, Price Steady", The CoinTelegraph, Aug 2017, https://cointelegraph.com/news/ethereum-breaks-blockchain-transaction-record-price-steady.

become an issue. To mitigate this risk, BitClave could deploy secure P2P channels, using technologies similar to technologies used by Raiden Network[24] or Bitcoin Lightning[25].

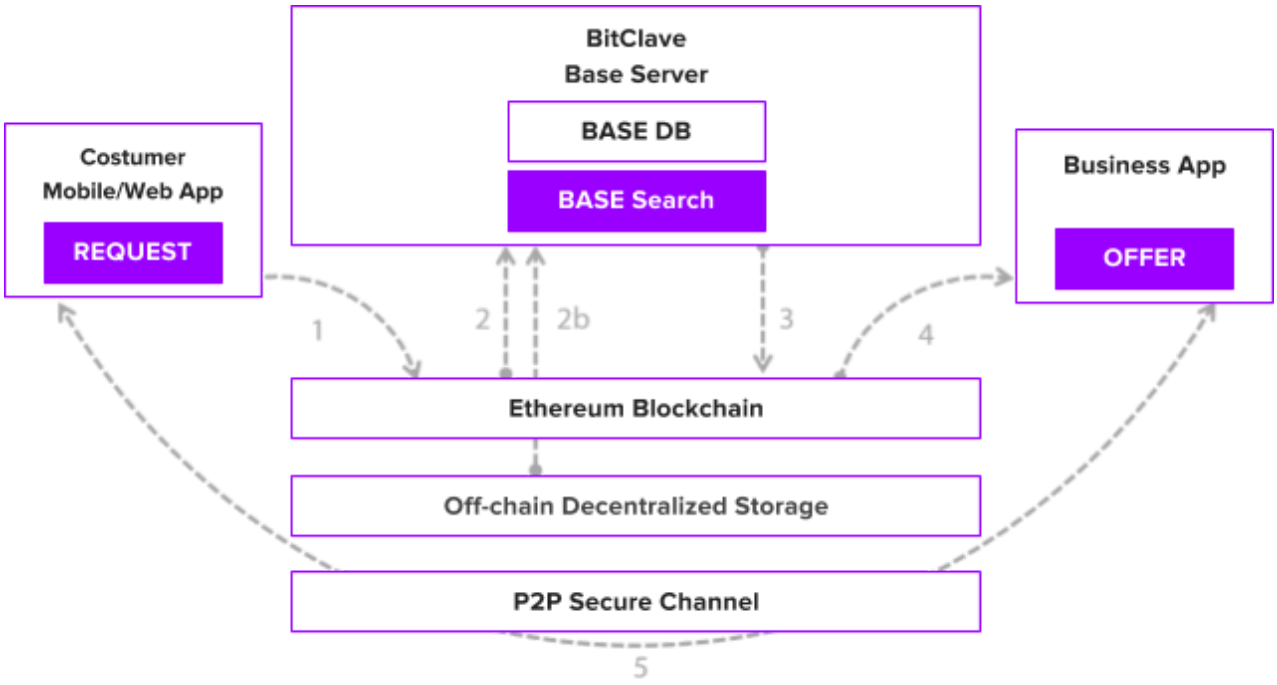


Figure 12: Direct P2P secure communication can be used to further offload some of the BASE interactions from the blockchain, improving performance and speed due to limitations of Ethereum.

As seen in the description of step#4, all communication is between REQUEST and OFFER, and the rest of the blockchain does not care about the details of this negotiation. What is important is whether the transaction happened or not, so we can use a direct "state channel" for step#5 and write only the final result to the blockchain. Furthermore, in case an OFFER is from a business that a customer is making continual purchases, the state can be stored off-chain for a longer period of time, until one of the parties decides to post the state to blockchain for global visibility. In this scenario, even more transactions are offloaded from the main blockchain.

Legal

BitClave is incorporated in Singapore as BitClave Pte. Ltd. and is headquartered and operated from California, USA as BitClave Inc. The BitClave headquarters, it's founders, and a significant portion of

[24] http://raiden.network/ - High speed asset transfers for Ethereum
[25] https://lightning.network/ - Scalable, Instant Bitcoin/Blockchain Transactions

development team are located in the USA where all federal, state, and local laws are obeyed and compliance enforced. To ensure legal compliance throughout the BitClave project and company structure, BitClave is working with leading law firms like Schiff Hardin and Cooley.

Additionally, we have added several key blockchain advisors including Guy Benartzi of Bancor, Chris Miess of TenX, Sten Laureyssens of Gambit Capital, and Min Kim of ICON, that are actively helping us implement industry best practices regarding the proper legal structure of ICOs in addition to advising on important business and technology related aspects of running a successful blockchain startup and building BASE.

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.

BitClave is also excited to announce a partnership with QTUM. Qtum is a hybrid blockchain application platform. Qtum's core technology combines the advantages of bitcoin core, an Account Abstraction Layer allowing for multiple Virtual Machines including the Ethereum Virtual Machine (EVM) and Proof-of-Stake consensus aimed at tackling industry use cases. What makes Qtum a viable option for enterprise-level blockchain applications, like BitClave's Active Search Ecosystem (BASE), is the ability to use Proof of Stake as a consensus mechanism. The more the network is used, the higher the volume of transactions, the more energy required to achieve true consensus. Proof of Stake gives an opportunity to build blockchain solutions capable of handling a higher transaction throughput, ideal for businesses and high-activity ecosystems like BASE

Initial Development Efforts

The initial design of the platform will be based on the REQUEST 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 REQUEST 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'll also implement VIEW activity to support "Proof of View" and CAT transfer from business to customer for viewing the OFFER.

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

As of middle of Oct 2017, there is an alpha version of the product. The alpha is currently under internal testing and will be released to a wider audience end of Oct 2017, before ICO start. The product will be released in 2018

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. 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 have already introduced 15-20 small companies for the initial instance of the BASE market. Our team will continue to target industries where significant effort is put into marketing to individual customers, such as auto sales, real estate, hotels, and retailers like Target that compete with major ad service providers like Amazon. Once our small market is established, we will increase our marketing efforts to continually expand the number of players involved.

New Opportunity

BitClave designs and develops an 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.

Fundraiser And Token Distribution

The ERC-20 tokens will be distributed no later than 4 weeks after the end of the token sale.

Fundraiser Schedule

To date, we have successfully completed a discount token pre-sale event. The full crowdsale is beginning on

November 29th. The fundraiser will continue until the hard cap of 25 million USD is met (or for 60 days). The official start date will be announced through official BitClave channels. Register at fundraiser.bitclave.com for the latest announcements regarding the fundraiser.

Token distribution

The ERC-20 tokens will be distributed no later than 4 weeks after the end of the token-sale.

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 openhanded 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

The BitClave 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.

Blockchain Developer, Anton Bukov

MSc from Institute of Cryptography, Telecommunications and Computer Science. Expert in data security and processing. Blockchain enthusiast and developer

Senior Developer, Ivan Yurin

Lead backend developer, experience with scalable systems

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, Min Kim

Co-founder of ICON Foundation. Chief Strategy Officer at DAYLI Financial Group. Partner at DAYLI Venture Capital.

Strategy Advisor, Alex Shin

Partner at BlockchainPartners Korea. Head of Operations at TeamBlind Product, User Aquisition/Growth.

Blockchain Advisor, Greg Wolfson

Entrepreneur and Blockchain expert. Former Director of Business Development at BTCC

Blockchain Advisor, Lucas Hendren

University of Illinois Alum Double Major in EE and CS and Physics. Blockchain entrepreneur and expert. Cofounder at SimplyVital Health.

Legal Advisor, Doug Park

PhD Stanford GSB, JD Michigan. Expert in corporate governance, business models, regulatory strategy, and organizations.

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.

Strategy Advisor, Enrico Ferro

Head of the Innovation Development department at Mario Boella Institute (ISMB). PhD from Politecnico di Milano.

Legal Advisor, Reza Dibadj

Harvard JD and MBA. Expert in solving complex problems in business law and business strategy.

Science Advisor, Brad Gaynor

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

Strategy Advisor, Elie Galam

Chief Investment Officer of the Eastmore Group. Masters in Applied mathematics Harvard University.

Glossary

Activity

An action in BASE that is recorded into Anonymized Activity Ledger. Activities include both online actions (e.g., search request, view of personalized offer, online purchase) and in-person actions (e.g., visiting a retail store or buying a product). Activities may be associated with customers, businesses, or both (see Activity Definition).

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 (also referred to as Active Search or Decentralized Search. See BASE Definition).

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 Ranking and Anonymization).

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 in BASE).

Follow us

http://www.bitclave.com/

 info@bitclave.com

 https://github.com/bitclave

 https://twitter.com/bitclave

 https://www.facebook.com/bitclave

 https://linkedin.com/company-beta/6399312/

 https://slack.bitclave.com

 https://t.me/BitClaveCommunity

 https://www.youtube.com/channel/UCtibs4mNHqbPn-NGnFtK6yg

 https://bitcointalk.org/index.php?topic=2005370

