A collection of decentralized, encrypted, event-driven, peer-to-peer (DEEP) node clusters, built on an adaptive mesh edge-computing network (AMEN) that records data through distributed and immutable ledgers using Write Once Read Many (WORM) storage.

DRAFT

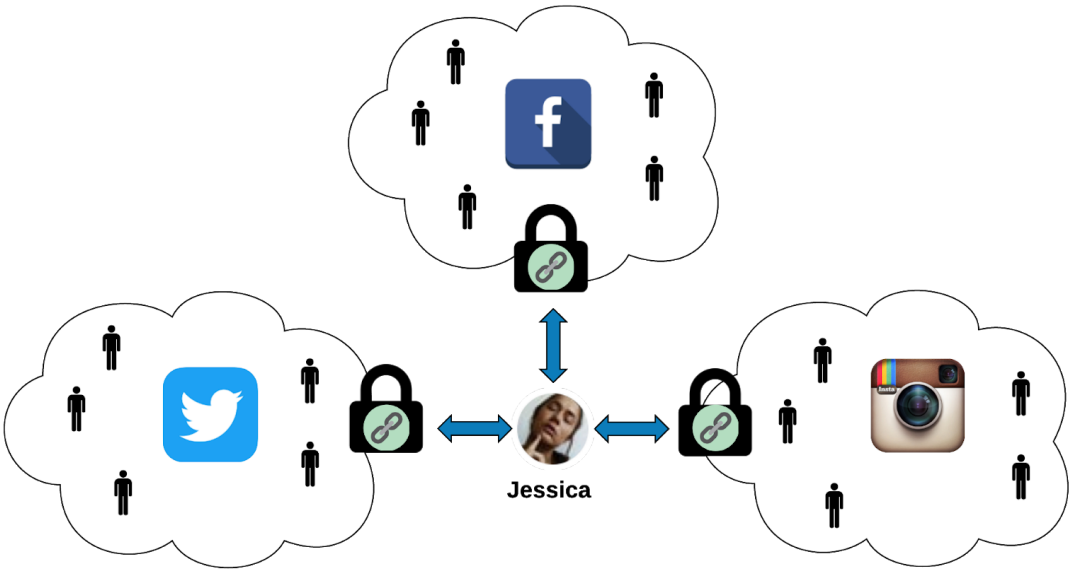
Version 1.0 (35)

Problem Statements

The Cloud is good for Business, but bad for Social

The centralized structure of cloud-based, social media solutions is an unnatural environment for individual social interactions to occur.

Traditional social media like Facebook is one large, two-billion person, centralized public network where all the users are members of a single “Cloud”. The Facebook mobile application is essentially a browser, which allows Facebook members to view their content stored on Facebook’s cloud servers.



In 1990, anthropologist Robert Dunbar proposed that there was a natural limit to the number of stable relationships any human being could maintain. Dunbar’s number limits each of our “real” social networks to 150 people. Therefore, joining networks like Facebook or WhatsApp that push their user base to follow accounts beyond Dunbar's number is hardly natural.

Cloud-based social media’s entire reason to exist is to exploit user data for profit, but it’s now increasingly responsible for manipulating information, attitudes, and opinions among its users as well. In fact, Stanford University recognizes that Facebook is one of the most primary sources of misinformation today.

For example, it's been discovered that Facebook uses 2FA authentication to hoard more user data and Facebook copies your phone's address book to their servers to farm more user data.

Even social media's advertisers—the ones theoretically profiting the most from user data—are starting to leave networks like Facebook, citing their 'despicable' business model of user exploitation as the cause.

Social users Need and Want more control

Social media users have no control over where their data is stored, how it's secured, or how it's shared, and this is contributing to destructive phenomenon like fake news, political interference, post-traumatic stress disorders, and even death.

Facebook will not change this. Government will not change this.

Users must change this dynamic of exploitation and manipulation by demanding control and ownership of our data.

The only true way to do this is to decentralize the way we network, and shift the focus of the Internet out of the clouds and back to the person.

This is why we're building Peer — to give you a place to start taking back control.

The Peer project

Goal

Our goal is to build a secure communication and data-sharing solution using a decentralized architecture and encrypted ledger technology to give users complete control of how they are social.

Concept

Peer is based on three core concepts:

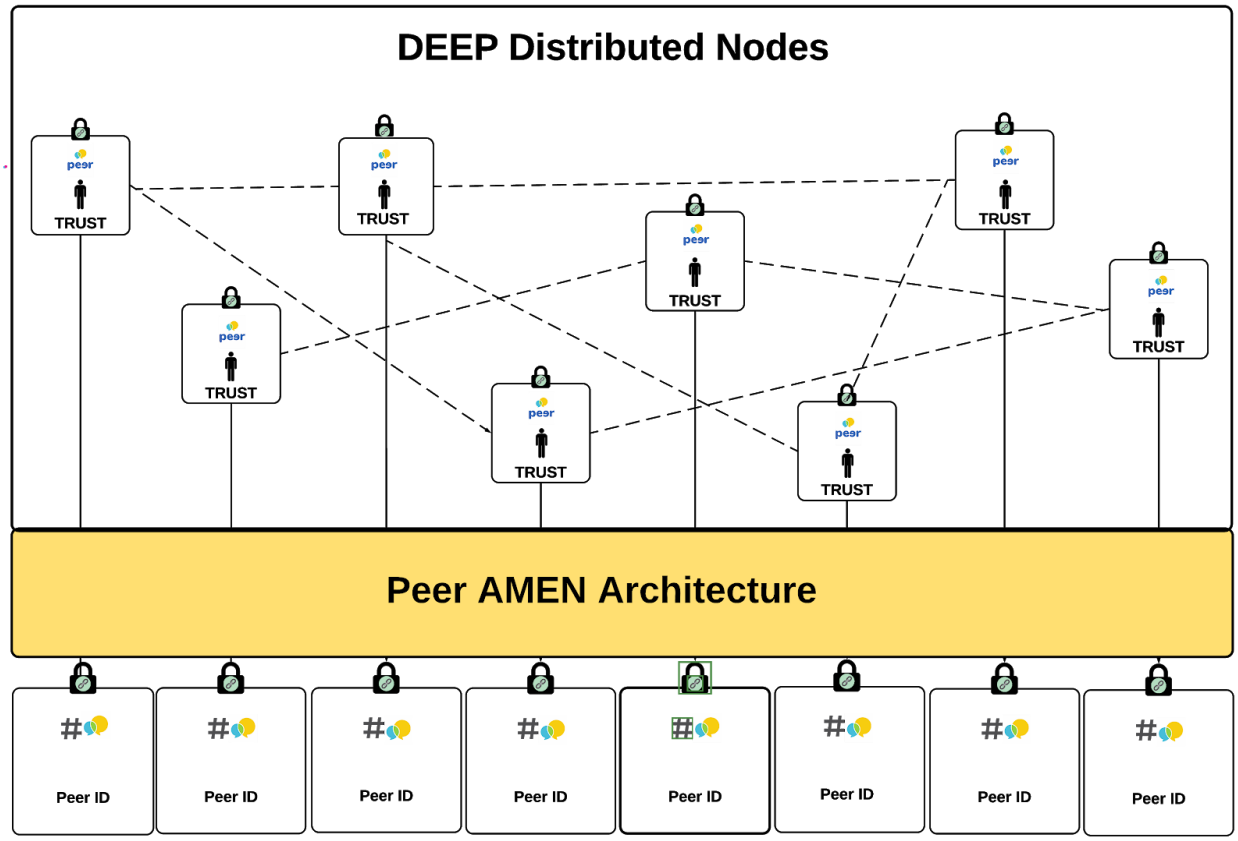
- **DEEP principles** – how we approach data distribution of node clusters
- **AMEN structure** – how Peer's network is organized
- **WORM storage** – how events, content, and communication are tabulated

Peer is a network of equally-privileged nodes with **D**ecentralized, **E**vent-driven, **E**ncrypted, **P**eer-to-Peer (DEEP) characteristics. To connect DEEP™ node clusters on the network we are using an **A**daptive **M**esh **E**dge-computing **N**etwork (AMEN) architecture to build a personal communication and data-sharing platform. Events are recorded through distributed and immutable ledgers using **W**rite **O**nce **R**ead **M**any (WORM) storage.

Every Peer user is a self-contained node in the Peer network, allowing complete, user-centric control of all in-coming communication presented on a self-moderated social newsfeed.

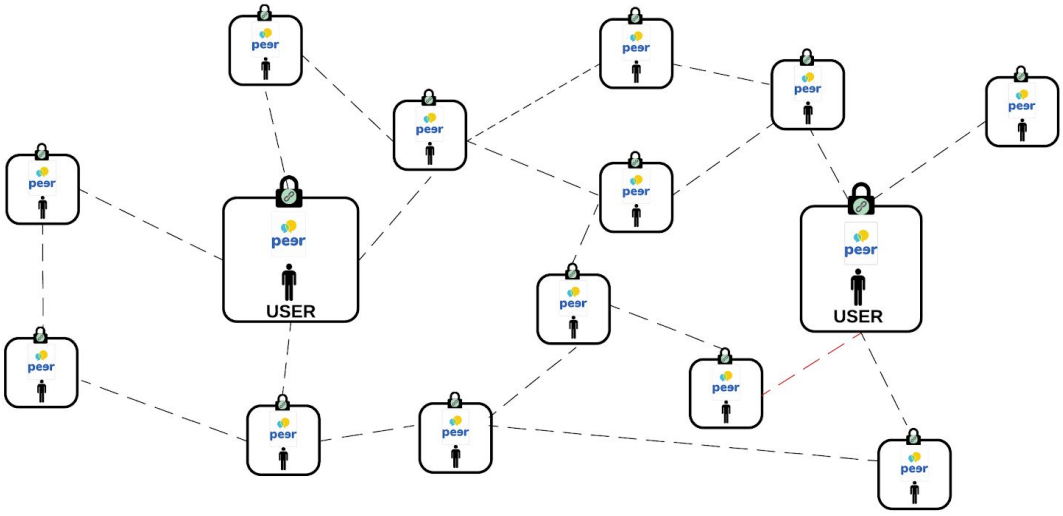
Peer is a decentralized network and no personal user data is stored centrally, so there's no way to centrally control what any individual user sees or does. Each Peer node contains the full technology stack necessary to build a secure, personal communication and data-sharing social network.

In an AMEN™ architecture, all nodes act as proxies for each other to account for times when a node is online or offline, allowing data to propagate in parallel between nodes. An AMEN architecture allows Peer to simulate centralized services, such as account recovery, in a decentralized network.



A Personally Encrypted Blockchain network

Every Peer user personally creates, controls, and stores their own immutable, ledger-based, adaptive network on their smartphone.



Users are represented by encrypted network node addresses, not names, email addresses, or telephone numbers. Usernames and passwords are stored locally on the user's smartphone so there's no centrally stored username and password lists for hackers to target.

Data and voice communication are relayed directly to and from other Peer users with whom they have shared public encryption keys. Each Peer node also contains a private, individualized, encrypted ledger that stores each connection and all subsequent communications as events.

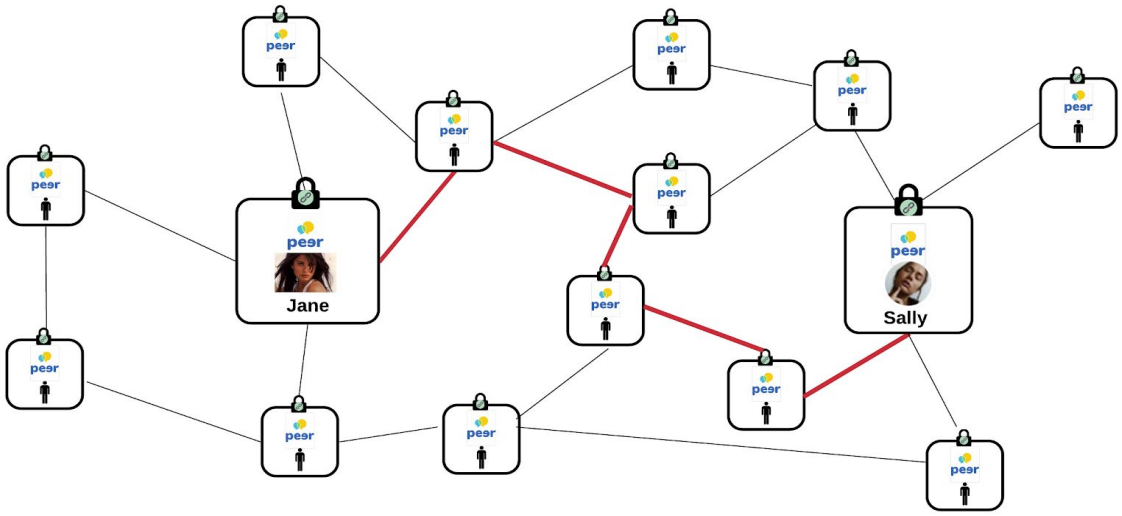
The decentralized world of Peer

A decentralized architecture means that nothing gets through to any Peer user unless they approve it by sharing homomorphic[1] encryption keys, recorded through distributed and immutable ledgers, between sender and receiver alike. This capability empowers Peer users to moderate their own newsfeeds and take responsibility for their social interactions on-line, while maintaining an adaptive world optimized for social interactions that align with Dunbar's number, ensuring the highest level of personal control.

Because of decentralization, it's important to understand that this adaptive world is not the totality of Peer profiles nor is it a silo of individual accounts. Each world is a cluster of peer nodes that re-distributes data through a limited degree of connections. Access to this data must

[1] Related to homomorphism, which means, in the mathematical sense, an into map between two sets that preserves relations between elements, according to dictionary.com.

be delivered from opt-in WORM storage across leaf nodes, emphasizing end-to-end communications.



Edge-computing, artificial intelligence, and machine learning

A key differentiator of Peer is the ability to harness computational power across diverse leaf nodes. Instead of being constrained by individual systems prone to limited storage and overheating (particularly with smartphones), Peer's edge-computing abilities balance toward sparsity of network traffic, as well as sparsity of data storage.

Likewise, because Peer engages in no user tracking to build and augment algorithms (motivated by surveillance), artificial intelligence and machine learning are used to determine which data is most relevant to a user's world. Peer is event-driven, therefore by applying edge-computing, we can more easily organize anonymized data across node clusters. Our technology stack is built to easily react to changes because it's adaptive by nature.

Hypothesis

Recent scandals have created a sense of fatigue among social media users and the endless media maelstrom that is the Donald Trump presidency only serves to magnify these feelings. Users have had enough of the relentless, ad-based exploitation of social media, and they're ready to quit or try something different.

Cambridge Analytica was the scandal that opened the floodgates against Facebook, but let's not forget that Cambridge Analytica styled themselves as a political advertising agency. People knew that selling Facebook user data to a political firm with the intent of influencing Brexit in the UK and calling it "advertising" was the last straw.

As punishment Mark Zuckerberg personally lost $4.9 billion the first day Facebook stock began trading after the Cambridge Analytica breach was revealed.

Even social media's advertisers—the ones theoretically profiting the most from user data—are starting to leave networks like Facebook, citing their 'despicable' business model of user exploitation as cause.

Social media users are concerned that their personal data is not secure and certainly not private. Recent scandals have proven that social media companies cannot or will not control how, and by who, their users' data is exploited.

- In March 2018, Cambridge Analytica breached 87 Million Facebook user records and in October, 2018, the UK fined Facebook the maximum £500,000.
- Unnatural sized social networks also provide a platform for users to exploit other users as was proven by $757,000 in fines levied against Floyd Mayweather and DJ Khaled for illegally promoting Cryptocurrency ICOs on Twitter and Facebook.
- On March 19, 2019, MySpace announced that they had lost 12 years' worth of pictures, videos, and digital music files in a server migration.
- On March 21, 2019, Brian Krebs broke a story that up to 600 million Facebook users login credentials were stored in a text file that was readily accessible to over 20,000 Facebook employees.
- Culminating in the European Union taking the unusual step of passing Article 13 to make it the social media company's responsibility to ensure and protect the digital copyright rights of all of their Euopean users. Technically this could even apply to displaying snippets of someone's post in a search result.

Complying with Article 13 and the new regulatory environment caused by Cambridge Analytica—and the resultant fallout—will cripple social media companies and change the online revenue generation model forever.

Social media users are now aware that their personal data is worth a lot of money to social media companies. As a result, more users are demanding to know how their data is being exploited, by whom, and for how much money.

We strongly believe that a personal communication and data-sharing network based on the latest secure, decentralized, ledger-based network technology is the solution to the myriad of problems facing today's Internet users and today's social media companies.

The fundamental issue facing social media and the Cloud today is the erosion of users' trust. Repeated data breaches, fines, and the broken promises of 2019 have left users, governments, and businesses looking for a solution. The only solution is one where the user has 100% control over their data and communication by design.

Decentralization is the only solution.

Quantitative Market Research

To confirm our hypotheses, Peer worked with Majid Khoury Research in Vancouver, BC, to reach out to 1514 Canadian social media users through a weekly Maru/Matchbox omnibus survey on June 13 and 14, 2018. We asked users three questions about their perception of the privacy and security of their information on social media.

Survey participants were asked to indicate how strongly they agreed or disagreed with the following statements using a scale of 1 to 10, where 10 is strongly agree and 1 is do not agree at all:

1. I will use a new social media platform if it provides me more control over how my information is being used by the platform.
2. I am concerned that my personal data on current social media platforms I use is not secure.
3. I am concerned that my personal data on current social media platforms I use is not private.

We also asked two questions intended to identify if users were starting to perceive that their data had value.

1. I would prefer a social media platform that gives me the option to make money from my personal information that I provide to the platform.
2. I am interested in a social media platform where I pay a subscription of $1.00 a month in return for not having to provide my personal information.

Results

The Maru/Matchbox Omnibus survey returned some interesting results. Half of the people surveyed (rated 10, 9, or 8 out of 10) are concerned their personal data on social media platforms is not private (49%) and/or secure (49%).

The scores were statistically higher among those aged 45+ with 56% agreeing, compared to 45% for younger groups.

A couple of interesting notes about younger users that came out of the survey include:

- Younger users seem less concerned about privacy and security, but are more inclined to try a new social media platform if there are financial incentives for providing personal information with 35% agreeing (rated 10, 9, or 8 out of 10) compared to 22% for older groups.
- French-speaking residents of Quebec seem more receptive to the idea of a new social media platform that provides more control over information, having the option to make money from personal information provided, and paying a subscription fee of $1 per month for not providing personal information.

Concerns over privacy and security of data are not new but concerns over lost value for data and unethical business practices at social media companies are. Peer addresses all these concerns so we moved on to a more in-depth, moderated qualitative analysis of social media users to see if they agree.

Qualitative User analysis

Qualitative analysis is the best way to determine user attitudes and position potential solutions because it's a moderated discussion. To conduct the qualitative analysis, we engaged Upwords—experts in online qualitative analysis for big brands like Molson-Coors, Maple Leaf Foods, and Unilever.

The Upwords team worked together with Majid Khoury Group to design a 45-minute online qualitative survey to identify key pain points with current social media and to introduce Peer as a solution. We expanded the scope of the online analysis to include target market users (+45 Facebook) outside of Canada and included some people outside the target demographic to see if we could find additional users for Peer.

The Upwords qualitative survey ran from September 18 to 22, 2018, and a total of 28 social media users from around the world were surveyed.

Unaided Feedback

Some of the best feedback we received from the Upwords analysis was "unaided". Unaided concerns about social media were focused on privacy and targeted content.

- **Unaided**, some expressed concerns about **privacy**.
    - Data mining and selling of personal data for corporate gain; wanting more transparency especially from Facebook.
    - User control and/or protection of personal information and content.

  "I wish Facebook did not mine/sell my data. I would be willing to pay a monthly fee for a social media solution such as Facebook if I had legal assurance (and recourse) that the company does not sell my data and that my pictures and content remained proprietary to me."

  (Female, Age 46, Canada)

- Others were more concerned about data mining especially related to **tracking behaviour**, and **targeting content** and advertising.
    - For these participants the concern was more about targeted content and, therefore, "mind narrowing" or creating viewpoint silos feeding into cultural segregation.
    - Many wished social media platforms, especially Facebook, were ad free.

“One issue that I have with social media right now is the over personalization of feed. I think it keeps people in silos of like-minded people which can be good but it creates a very specific lens from which to perceive the world which, I think, contributes to segregation.”

(Female, Age 54, Canada)

- Other concerns focused on **more interface control** and/or **the elimination of negative influences** in social media (trolling, fake news, “keep the stupid out”, using the anonymity of online to be nasty, and so forth).

“I wish I somehow could get rid of all the fake news. Fake news is going to kill democracy or at least undermine it substantially. I've got friends that no longer believe in public statistics ‘cause they think it's manipulated to fit a specific cause and because of that they now are looking at the extreme groups all because of fake news. Scary... Getting rid of fake news would make life so much easier.”

(Male, Age 51, European Union)

Aided Feedback

One of the great things about qualitative analysis is that there are no right or wrong answers, as feedback is encouraged throughout the moderated engagement.

Unaided feedback is best because it comes from a place of honesty, however “aided” feedback is valuable as well. When provoked by the Upwords moderator, most were concerned or very concerned about privacy.

Specific user concerns included:

- Personal data **accessible to third parties without consent**
    - Leading to targeting of content/advertising/AI predicting behaviour
    - Lack of clarity or knowledge about how personal information is being used and/or concern about what unknown entities may know
    - Identity theft
    - Potential for fake news and/or doctoring of information
- Facebook, specifically Cambridge Analytica
- Many were already taking action to thwart privacy concerns **by being careful about the content they pos**t; **exercising control over posting or settings**.
    - A few are using aliases
- For a few, there was **a sense of acceptance**—social media is not private.
    - Those who were less concerned, felt a sense of acceptance.
    - Some felt more concerned about Facebook than other platforms such as Instagram where the interactions felt less public.

User understanding of Peer concept

The first part of the 45-minute qualitative analysis was focused on getting a deeper grasp of the market for a new type of social media application.

In the second part of the qualitative analysis, we tested the Peer App concept statement, specifically by asking them what they understood about Peer after reading the following statement.

> “Do you love being able to connect with friends on social media, but dislike the idea of your network being controlled by large corporations seeking to profit from your connections and activity?
>
> Introducing Peer—the social media network made personal. Peer is YOUR private social media network.
>
> Peer is the ONLY social media network of its kind. You build it how you want, you store it on your phone, and you control it. Peer is maintained and run by users with no algorithms and no unwanted advertising. Peer is 100% you!”

Peer was well understood as a social platform focused on increased user control, data privacy, and protection without unwanted advertising or corporate control.

> *“There is a new social media site that is not operated by a corporation, but is controlled by the user. It is private and there is no risk of your information and statistics being used by anyone.”*
>
> (Female, Age 46, Canada)

> *“Peer is a social network you build yourself--you control it and can personalize it. It doesn't have additional ads.”*
>
> (Female, Age 55, Canada)

> *“Hey, I heard about a new social network that you may like more than FB because it offers control, privacy and no ads.”*
>
> (Female, Age 50, United States)

> *“Social media app that we fully control - no ads, targeted commercials or exploitation of our data.”*
>
> (Female, Age 26, Canada)

> *“[Peer] is a terrific Social Media App that has no advertising, does not share any data, and is 100% configurable by you. In fact, it is 100% user driven.”*
>
> (Female, Age 54, Canada)

“Imagine using an app that would allow you to build and stay in touch with your own communication network…Imagine that you can manage your own universe - in real time.”

(Female, Age 69, Canada)

Conclusion

The combination of quantitative and qualitative user research proves our hypotheses that social media users are concerned enough about the privacy, security, and value of their data to leave social media like Facebook, and they’re looking intelligently at any alternatives like Peer.

Recent scandals have clearly created a sense of suspicion among users of all things Social. This is why another centralized, cloud-based solution will not fly. To change Social, the solution **must** be 100% user focussed—the **only** way to do this is with **decentralization** and users know it.

Peer is the solution.

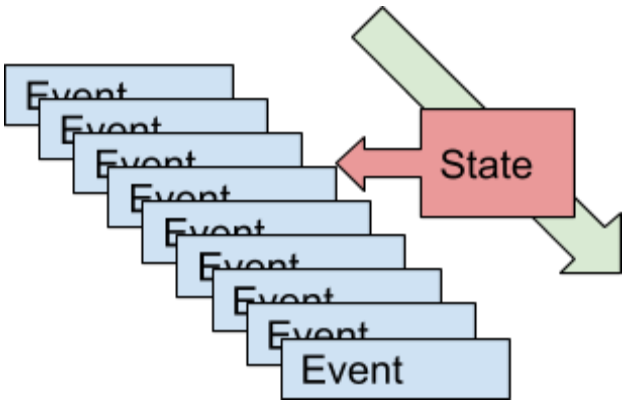
Method

At Peer we are building a cutting edge solution so we need to use cutting edge methodologies, systems, and technologies. Starting at the architecture level, Peer will be built using Event Sourcing, a development methodology built for decentralized systems.

Event Sourced Architecture

Event Sourcing mandates that public posts, direct messages, or posts to private groups are recorded as events on WORM (write once, read many) drive the type of storage.

The core of integrity of state is being able to ensure order and durability. Concepts from Greg Young's Event Store accounting-based architecture are used in the Peer mobile platform. Using an accounting-based architecture allows Peer to have data integrity by design, not by attaching multiple, discreet database tables to multiple systems.



Accounting-based architecture is also best suited where systems require scalability and transactional integrity. In certain circumstances, partial centralization (caching) of data is required in distributed systems to ensure transactional integrity. Using Event Store allows Peer to accommodate ever-increasing needs for data caching by design.

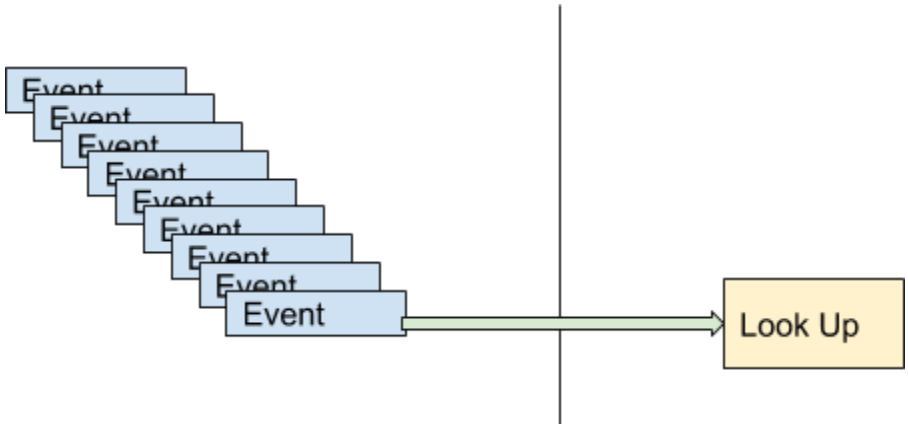
Event Store powers Walmart.com, LineData, and air traffic control systems among many other solutions around the world. Event Sourcing in tandem with other technologies enables Netflix, LinkedIn, eBay, and it's the recommended way to scale distributed data systems by Amazon's whitepaper on the subject.

Using Blockchain technology

The Peer event sourced architecture creates events that are recorded in an encrypted ledger, stored in an encrypted folder on the user's smartphone. Using an encrypted ledger to store the state of a connection between any one Peer user and any other Peer user allows us to

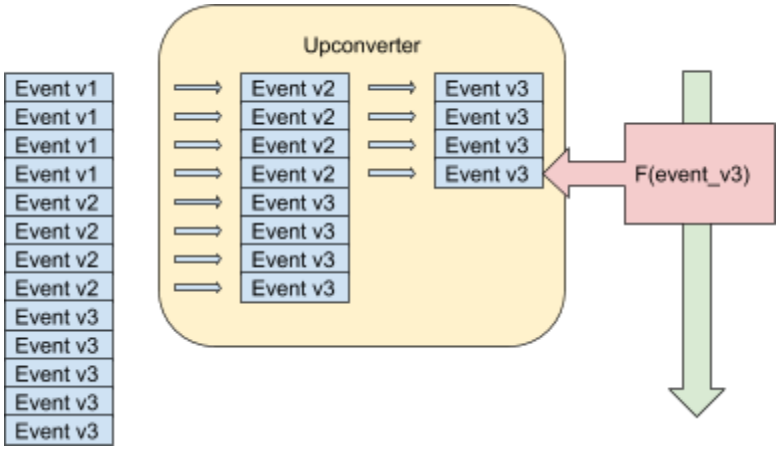
guarantee the authenticity of any connection. More importantly for Peer users this also means that users can modify or break any connection, any time, by changing the event state.

Subscribing to external events and presenting state of other nodes is the integration pattern used by Peer to allow for a single source of truth to govern the projections of what information the users are presented and, more importantly, what information they're basing their actions on.



Open Standards and Upconverting Conventions

As Peer evolves, so does the structure of the data. By ensuring an immutable ledger approach to append-only storage, there's a reliable way to interpret previously stored information to current implementations.



At its core, Peer applies fundamental, accounting-like, data management strategies along with open-standards to avoid obsolescence and proprietary formats, thereby avoiding future vendor lock-in and preventing technological obsolescence.

Adaptive Mesh Network Data Distribution

At its core, Peer needs to accommodate a level of mobility that can match human-to-human information exchange. The fundamental test of the ability to manually enter information from a stream into the application always succeeds. As long as the encryption signatures check out, the user can rely on the information as having been secured by the Peer digital infrastructure.

Building on this, Peer uses a friends-of-friends, fanned out network structure to distribute a cache of content to maintain continuity of the data and provide the same experience as a Cloud solution. As the demands of larger networks or super users proliferate, non-actor nodes are available to facilitate indexing, cache-invalidation, and other aspects needed for distributing information outside of the scope of Dunbar's number.

Projecting availability of certain nodes in a 2-degrees-of-separation fan-out is driven by adaptive system implementation that evolves with the maturity of Artificial Intelligence and Machine Learning, and is in place to facilitate the most up-to-date view of the users' network posts.

Non-Actor Nodes

The performance and on-demand content of centralized Cloud-based solutions is facilitated on an as-needed basis. This could be an interest group like panorama photography enthusiasts and the content is available with the paradigms in regular cloud solutions, with the added feature of being encrypted.

Homomorphic Encryption

As the field of cryptography evolves, the ability to process encrypted data to offer state transitions without compromising data sovereignty will be at the core of distributed computing. Peer is built on a topology and approach that adapts to leading-edge innovation in cryptography and offers the best assurance for privacy and data ownership.

Conclusion

We're confident that the time is right for a disruptive change to the way people create and interact with their online community. Data shows that users will easily join social networks if there's a compelling enough feature that cannot be found elsewhere. This requires a radical

re-think of the Cloud-based architecture and the advertising-based business model of traditional social-based networks.

The solution must give the average Internet user confidence that their data is secure and under their control.

The solution must also provide a secure and private infrastructure that accommodates mobility and the low-latency services we've come to expect from mainstream communication and social-based solutions.

We believe Peer has the right combination of new technology and new thinking to be that solution.

Technical Glossary

Term	Definition
Adaptive	The ability to change the connections used to communicate and exchange data on a mesh network depending on the effectiveness of each node as a participant on the network. This ability is needed due to the need to scale across different network densities.
AMEN	Adaptive Mesh Edge-computing Network; the structure of our Peer-to-Peer network.
Anonymized	Encrypted data that's not readable by other nodes that don't have the keys to unlock it.
Architecture	A paradigm of information design
Artificial Intelligence	Any device functioning as an autonomous entity that perceives its environment and takes actions that maximize its chance of successfully achieving its goals.
Blockchain	A group of records that are linked using cryptography and often contain a cryptographic hash, time stamp, and transaction data (dependent on the network effect in the user's world—once written, cannot be erased).
Credential	Attestment to access control of information or other resources.
Decentralization	In information technology, any platform or architecture that has a high level of independence from a governing authority, and encompasses both intermediate and end-to-end communications.
Distributed	Copied to connected nodes for various purposes.
Distributed ledger	A distributed consensus of data that is spread across multiple devices, sites, and institutions.
DEEP	Decentralized Encrypted Event-modelled Peer-to-peer; the very principle upon which we've built Peer.
Dunbar's Number	A suggested cognitive limit to the number of people with whom one can maintain stable social relationships (see world).

Edge-computing	Distributed computing paradigm that stores computer data and functionality across device leaf nodes (implied connections), and processes computation across machine clusters.
Encryption	Encoded communication, messaging, and information that's accessible only to authorized parties unlockable by cryptographic key.
Event	Transactionally bounded change of state marked by an action undertaken by a user or automation of a system. Events are taken as fact to build a common source of truth.
Event-driven	A method of reacting to state changes that can be internal and external to the system.
Event-sourced	An agreement about using ledger as a source of truth.
Fanned-out network structure	The bounds and scope for the subset of nodes that comprise a user's world.
Homomorphic encryption	A form of encryption that allows computation on ciphertexts, generating an encrypted result that, when decrypted, matches the result of the operations as if they had been performed on the plaintext.
Immutable ledger	An additive-only way of keeping account of state in the spirit of double entry bookkeeping, but in the realm of information systems.
Leaf nodes	An infrastructure node that's the endpoint of information that comes from large-scale, intermediate, centralized network infrastructure.
Ledger	An account of what happened
Machine learning	Algorithms and statistical models that computer systems use to effectively perform a specific task without using explicit instructions, relying on patterns and inference instead.
Mesh	A method of networking in which nodes connect directly, dynamically, and non-hierarchically to each other.
Network	The method by which the user's world is connected and facilitated through trunk, subsidiary, local, topological infrastructure.

Node	A redistribution point or communication endpoint, paired with the user, often associated with networked devices such as servers, routers, computers, and smartphones.
System	A closed set of components that collaborate for functionality. For Peer, this is internal to the device owned by the user.
Technology stack	A set of standalone software subsystems or components to create a complete platform that delivers functionality.
World	For purposes of network effect, the world to the user is the Dunbar number to the 2nd degree.
WORM	Write once, read many; this storage is incorporated in our Peer design.