Mesher White Paper

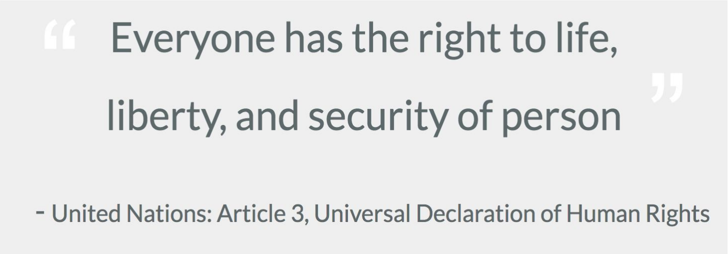
February 2018

Abstract: Mesher is a decentralized application framework, designed to facilitate individual ownership and control of user data, targeted at children.

Background

Since Bitcoin was announced in 2008, there has been a proliferation of blockchain platforms designed to facilitate the scaling and development of decentralized applications. With the exponential growth of user and machine-generated metadata, and the increasing sophistication of encryption technology, blockchain platforms are an increasingly attractive solution to solving critical issues around secure ownership and storage of user data.

Virtual Rights



> “Everyone has the right to life, liberty, and security of person”
>
> - United Nations: Article 3, Universal Declaration of Human Rights

The concept of Rights is one we have all grown up with. The right to physical property and bodily autonomy. The right to freedom of speech, and freedom of association. We generally agree that Rights are a pro-social good; rights form the basis of our individual defense against coercion and tyranny, allow us to engage in transactions of mutual benefit, and help to ensure that the benefits of cooperation and networking are distributed widely, rather than concentrated in the hands of a violent few. Rights form an articulate basis for ending slavery, and tackling the cycle of poverty. The most acclaimed governments in the world are those with effective rule of law; that is, practical applications of rights that have been codified and executed in predictable and progressive ways.

New forms of human communication and interaction with technology require us to continuously adapt our conception of rights to new mediums. The rise of personal computers, smartphones, web services, and the

Internet of Things is bringing with it a proliferation of data that is exponential in nature: data generated by humans and our machines is doubling in size every two years or less.

Certainly, a reasonable defense can be made that a private service should be able to own whatever is created on it, and add or remove participants at their own discretion. Indeed, that's the operating principle and business model on which today's most profitable web services are based. However, with many social networks looking increasingly less like small gatherings in private living rooms, and more like open worlds in which we engage in activities with real-world implications, issues of privacy, security, and ownership are critical. The freedom of virtual interaction is one which requires supporting digital architecture in the same way that our physical rights require cohesive rule of law.

The State of Our Data

Today, the bulk of user-generated data is owned by large companies that we rely on to manage aspects of our virtual identities, with Facebook and Google being two of the most well-known examples. These large companies try to suggest they are not monopolies but Google owns 80% of world-wide search engine traffic[1] and combined, they own 73% of all digital advertising spend in the US[2].

These technology companies mine us freely for information at their discretion, provided we sign an initial all-encompassing opt-in waiver which we never read. When nearly all mainstream social networks run on centralized servers (or distributed server clusters), users are dependent on these private servers, and vulnerable to a host of threats.

Facebook and Google use this data (Figure 1) to understand your usage behaviors and generate revenue from it. Unfortunately, this is just the beginning as large technology companies own or have significant influence on a number of different companies and therefore, industries.

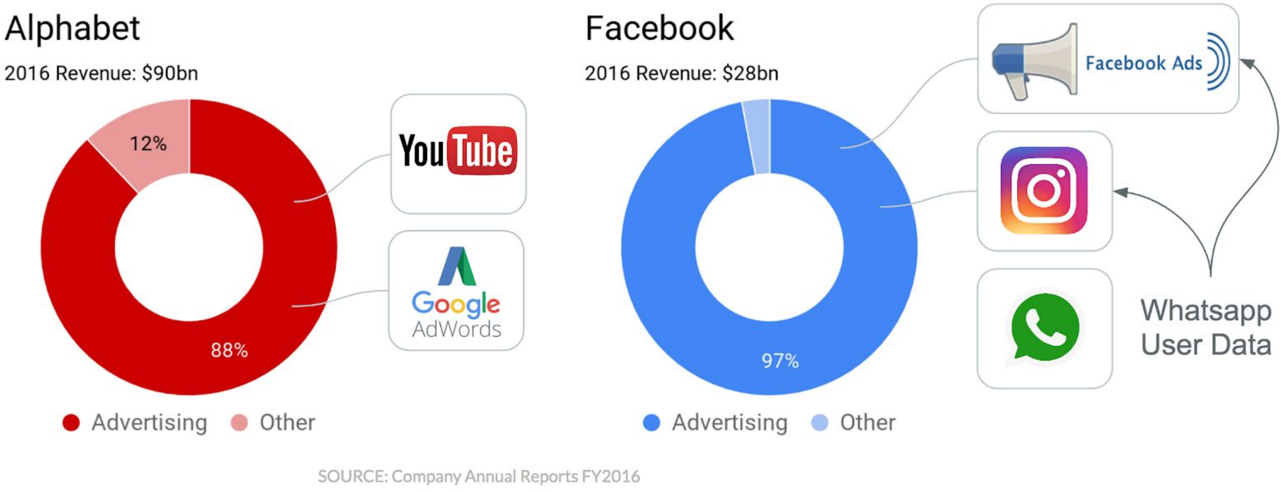


Figure 1: Data Usage Today

[1] Google search market share
[2] Google and Facebook digital advertising market share

In the future, with access to this level of information, they not only will continue to make money off of your created data, they can and are cornering other industries and becoming a larger, centralized store of data about you. They know who you are, who your friends are, what you've said to them, your interests, where you live, where you go, your mobile phone usage, your personally stored cloud data, what videos you watch, and access to health data (through DeepMind), which was assessed as legally inappropriate by the UK, plus access or control over significant amounts of other data. In addition, the can acquire their investments with all the money they have and further strengthen their dominance over industries[3].

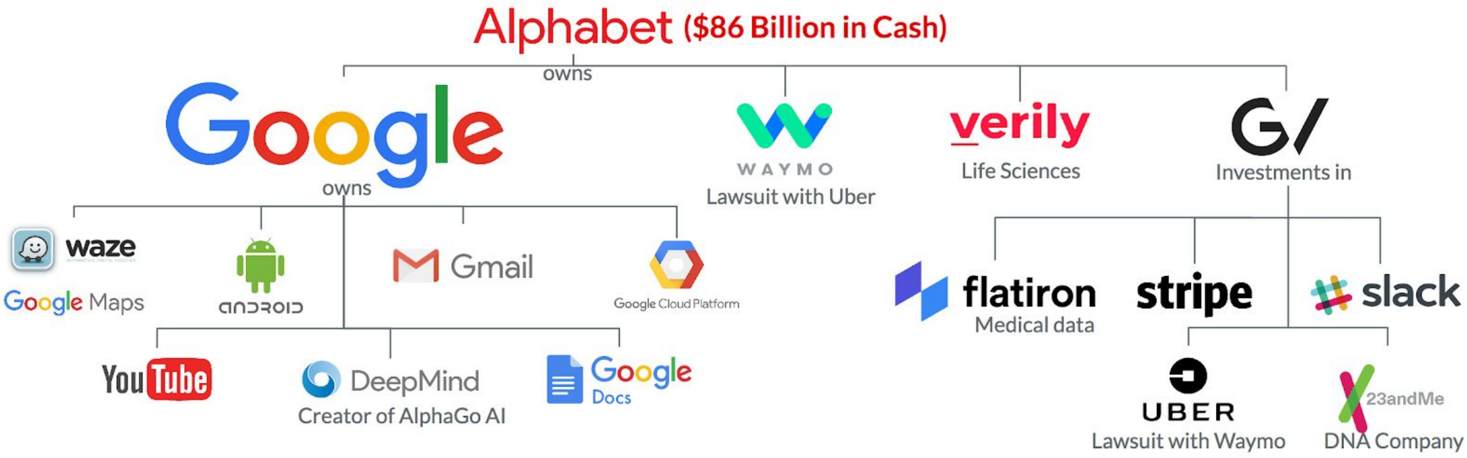


Figure 2: Data Usage in the Future

Breaches of Trust

These companies centralize all their data about you and thus become vulnerable to major hacks, putting your security in jeopardy. Over the past few years, some of the largest data breaches have been (Figure 3) companies such as Equifax, where over half of all Americans had sensitive data taken[4] and yet they didn't disclose the true extent of the breach[5].

[3] Alphabet's/Google's investment extent
[4] Largest data breaches of the 21st century
[5] Equifax under pressure after data breach update

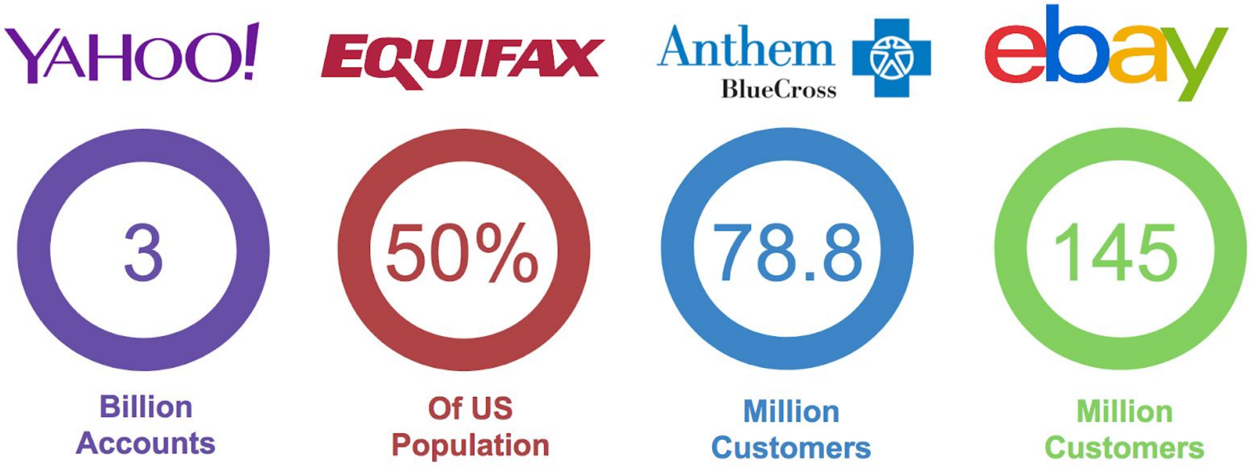


Figure 3: Significant Data Breaches

This has happened with Uber, where they took over a year to disclose their data breach[6] and combined, your SSN, credit/debit card data, addresses, emails, phone numbers, back account data, usernames and passwords, Government data, and medical company data were taken.

This is likely to occur again as hackers attack central authorities to obtain all this data and regulators are playing catch-up and companies such as Google and Facebook control more data about you and pose a greater risk[7]. Last year Google's parent company was slapped with a $2.7B fine for illegally promoting it's own price-comparison service in search results.

Worse still, educational systems have seen a 68% increase in data breaches from 2015 to 2016 and are making a larger percentage of total data breaches, from 7.4% of all breaches in 2015 to 9% in 2016 and a continued increase in 2017[8].

Introducing Mesher

Mesher is designed to facilitate individual ownership and control of user data, targeted at children. The barrier to owning and controlling our data ourselves is less a technical one, and more the challenge of overcoming user apathy, and achieving network effect while directly challenging multi-billion-dollar valuations by attacking the unfettered access to treasure troves of user data on which they are based.

In order to secure our Individual Human Rights in the Virtual Age, we need to build infrastructure which ensures we own and control our online identities and associated data. We can already facilitate peer to peer and hybrid networks that can benefit from both private and public interactions without requiring that we turn the entirety of our virtual lives and identities over to a third party.

[6] Uber data breach
[7] Forget Equifax, Google and Facebook have data you should worry about
[8] Data breaches in the US by sector

With the introduction of Bitcoin and blockchain technology, with it's continued developments, Mesher can leverage the blockchain to provide a secure, decentralized data ecosystem for individual ownership and control of user data (Figure 4).

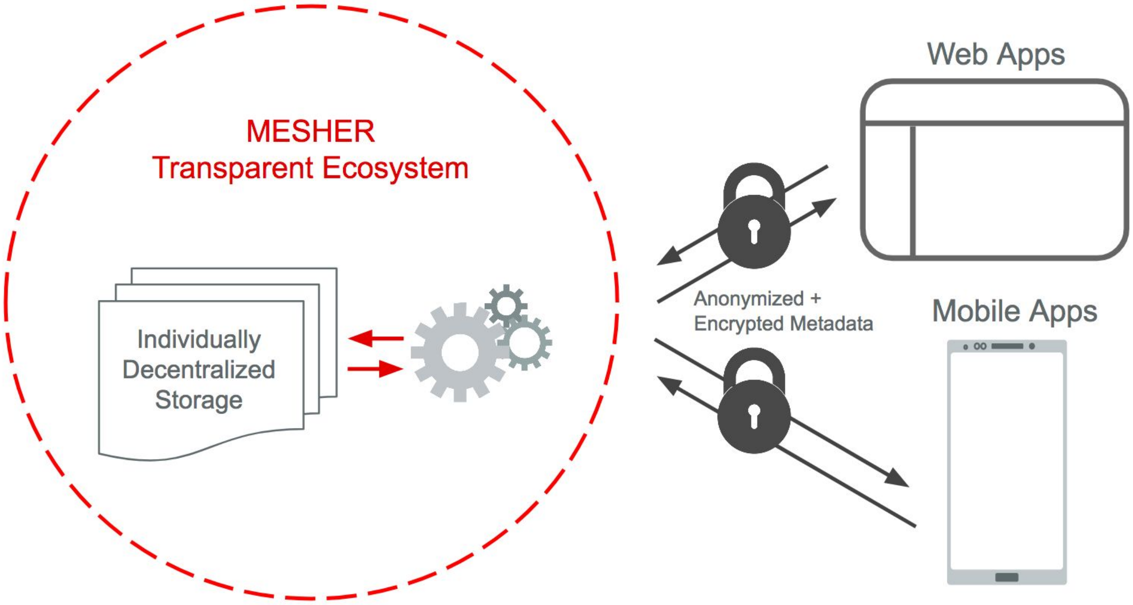
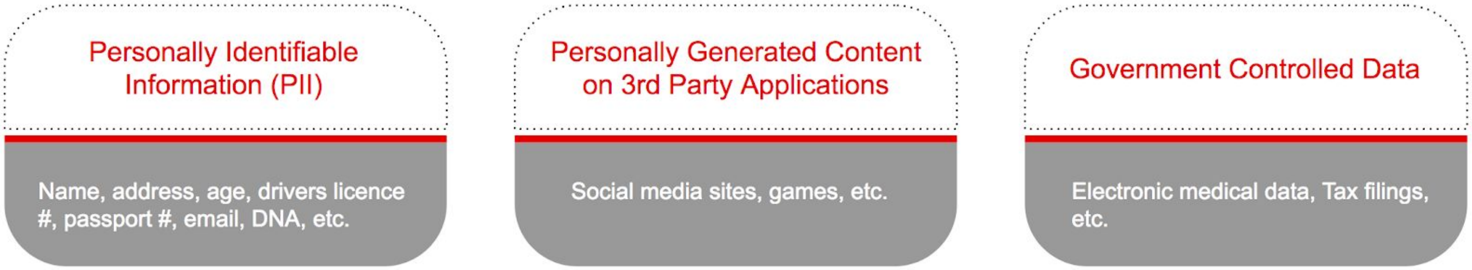

MESHER
Transparent Ecosystem
Individually Decentralized Storage
Anonymized + Encrypted Metadata
Web Apps
Mobile Apps

Figure 4: Mesher Blockchain Technology

Controlling Your Data

Control involves transparency over three types of data (Figure 5), personally identifiable information and personally generation data on 3rd party applications. They also need to know who is accessing Government controlled data about them.



Personally Identifiable Information (PII)

Name, address, age, drivers licence #, passport #, email, DNA, etc.

Personally Generated Content on 3rd Party Applications

Social media sites, games, etc.

Government Controlled Data

Electronic medical data, Tax filings, etc.

Figure 5: Types of Data Required to Control

Mesher Ecosystem

The Mesher ecosystem allows for interactions (using various extensions (Figure 6)) with numerous applications and can act as a login feature (without having to send username or password data) and can approve any data requests from the individual.

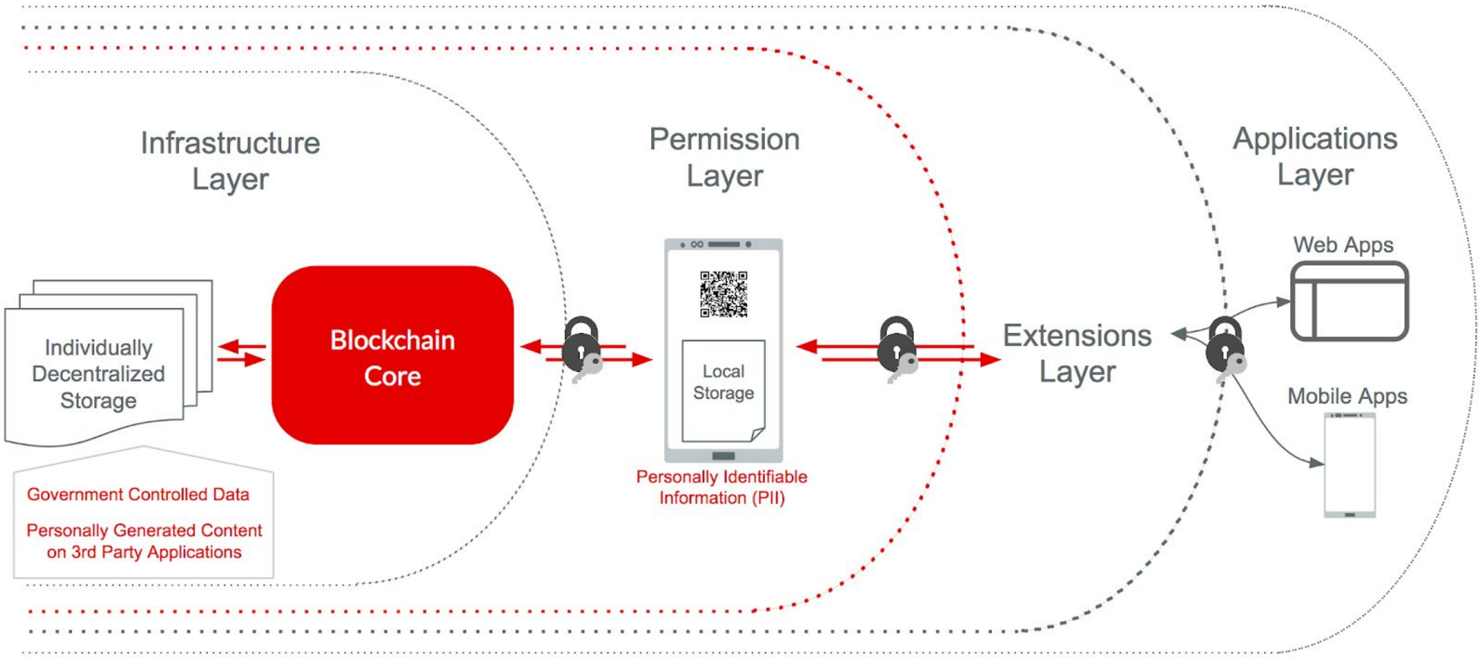
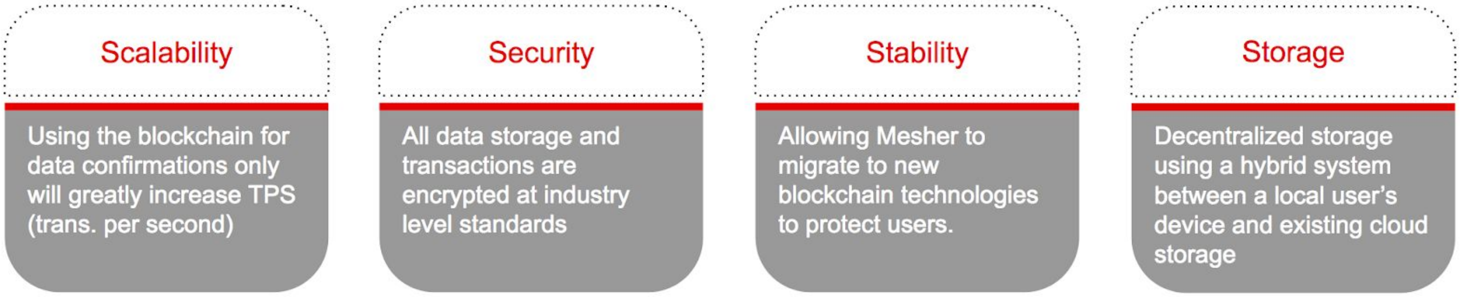

Infrastructure Layer
Individually Decentralized Storage
Government Controlled Data
Personally Generated Content on 3rd Party Applications
Blockchain Core
Permission Layer
Local Storage
Personally Identifiable Information (PII)
Extensions Layer
Applications Layer
Web Apps
Mobile Apps

Figure 6: Mesher Ecosystem

Mesher Infrastructure Requirements

In order for the Mesher ecosystem to be able to protect individuals' personal data, the infrastructure Mesher is built upon must meet the following requirements (Figure 7):



Scalability

Using the blockchain for data confirmations only will greatly increase TPS (trans. per second)

Security

All data storage and transactions are encrypted at industry level standards

Stability

Allowing Mesher to migrate to new blockchain technologies to protect users.

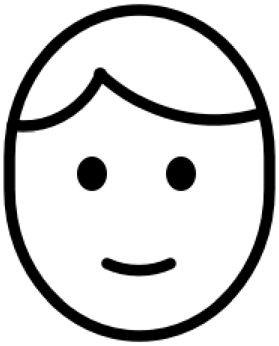
Storage

Decentralized storage using a hybrid system between a local user's device and existing cloud storage

Figure 7: Mesher Infrastructure Requirements

Young User Strategy

Most new technologies that achieve network effects (the phenomenon where increased numbers of users of a network or service increase it's value or utility) in a quick and lasting way do so by appealing to a younger, nascent market, at least initially. Facebook, for example, was built as a platform for college students, before being adopted by high schoolers and other young adults. Within a year of being launched, it soared past 1 million users. SnapChat, WeChat, Uber, Minecraft, and various other hot platforms similarly benefitted from the power and virility of user adoption in young markets. Mom, Dad, and Grandma often only follow suit at the urging of their children, or once they realized they will have to adopt the platform themselves if they wanted to keep in touch with their kids' regular activities.



Young users tend not to have barriers to testing out new systems and products in their leisure time that older ones do. Factors include more free time, less bias towards existing technologies, and a greater propensity to test out things quickly without regard for risk and downside. It is easy for a fun and useful product to go viral quickly amongst young well-connected peers who are often part of various fluctuating networks of schools, teams, and playmates. The biggest barrier and influence on the technologies children adopt, outside of their own peer circles, is their parents, and, increasingly, their educators. Many parents create guidelines to manage their children's interaction with technology, and many schools are now requiring that students utilize various applications, devices, or learning management platforms to supplement their educational experience. Since home and school are the environments in which youth spent the bulk of their time, their technological environment is still largely controlled by the level of access granted by their authorities.

The relationship between teacher and parent is one which requires communication and cooperation, so there is massive opportunity to create stronger interfaces between the two networks, and greater attention paid to the underlying network infrastructure and how the data generated by and about children is managed.

For Mesher, the natural target for implementing data management best practices should be in the environments used by young people that tend to allow for better management and control of mass implementation to achieve the network effect required to lead to lasting social change.

Mesher Roadmap

As with all blockchain startups, a strong infrastructure and users are the two most necessary requirements for a successful ecosystem. Instead of inventing yet another blockchain core, Mesher will be using existing public blockchain technology that meets the requirements set forth earlier. Since blockchains are becoming more of a utility, Mesher needs to ensure that users are protected and that the community is able to migrate from one public blockchain to another. Therefore, we will have a blockchain on blockchain (BoB) architecture whereby a permissioned blockchain layer will sit on top of a public blockchain.

The BoB architecture and building on a well known blockchain, with a large community, will allow Mesher to meet two of our infrastructure requirements, stability and scalability. Mesher's permissioned layer will move batched transactions on to the public ledger.

Phase 1:

Phase 1 (Figure 8) of the roadmap is to build and test the BoB architecture. Mesher is currently testing an internally developed, free application to allow parents and teachers to message each other, pay for school fees (such as field trips), and to allow calendar reminders to be sent to parents, all in one application.

Integrating payments, messaging, and calendar invitations in a free application will allow for early user acquisition. While the application is released, the application will be integrated onto the BoB layer to allow for a truly decentralized application for all the parties involved.

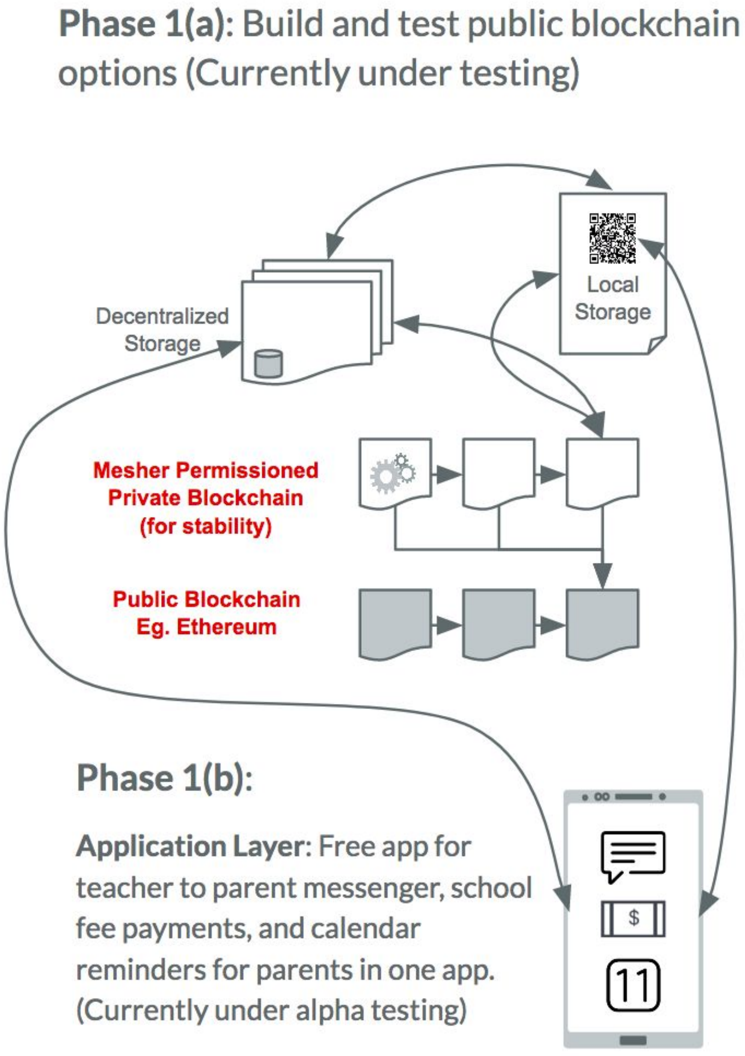

Phase 1(a): Build and test public blockchain options (Currently under testing)
Decentralized Storage
Local Storage
Mesher Permissioned Private Blockchain (for stability)
Public Blockchain Eg. Ethereum
Phase 1(b):
Application Layer: Free app for teacher to parent messenger, school fee payments, and calendar reminders for parents in one app. (Currently under alpha testing)
$
11

Figure 8: Phase 1 Mesher Roadmap

Phase 2:

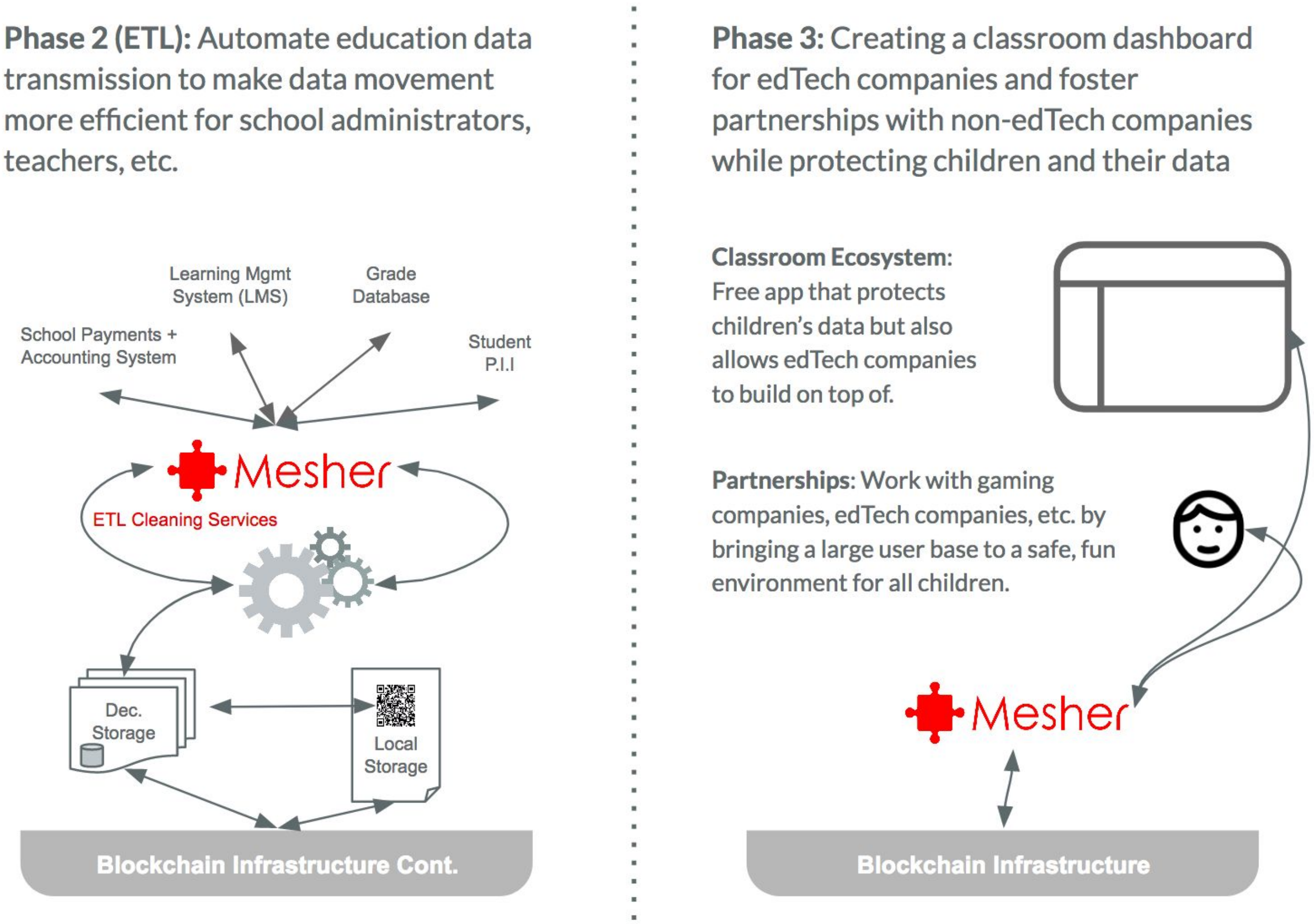
In order to increase adoption of the free application and the edTech ecosystem, Phase 2 (Figure 9) involves building out an ETL system to move data between all major education technologies (LMS, grade databases, school payments & accounting system, etc.). Having a well functioning ETL for educational institutions will allow existing edTech become adopted as the ETL will allow (with school administrators' approval) to pre-populate edTech systems such as learning management systems (LMS) and thus reduce the work required for a teacher to use existing or new technologies.

In addition, by offering the ETL service at a discounted price for underprivileged neighborhoods, we can help edTech reach all young people. Fees will be charged to edTech companies and thus, the cost of education will not increase for the families that may already have challenges paying for school supplies, etc.

Phase 3:

Phase 3 calls for the classroom dashboard to provide a self-serve system for edTech companies to work with school administrators to connect and build upon the Mesher infrastructure. To further adoption of Mesher's technology, we will be partnering with companies that require child-protection law compliance as a service. With a sufficient userbase, companies will be able to scale quickly due to the users the Mesher ecosystem would already have (note: parents will be able to monitor their children's activities as well as need to approve the use of 3rd party services).

While their are competitors in this space, Mesher plans to offer single sign on (SSO) in a decentralized manner, never have access to any edTech company or user's data, and allow for a higher level of security.



Phase 2 (ETL): Automate education data transmission to make data movement more efficient for school administrators, teachers, etc.

Learning Mgmt System (LMS)
Grade Database
School Payments + Accounting System
Student P.I.I
Mesher
ETL Cleaning Services
Dec. Storage
Local Storage
Blockchain Infrastructure Cont.

Phase 3: Creating a classroom dashboard for edTech companies and foster partnerships with non-edTech companies while protecting children and their data

Classroom Ecosystem: Free app that protects children's data but also allows edTech companies to build on top of.

Partnerships: Work with gaming companies, edTech companies, etc. by bringing a large user base to a safe, fun environment for all children.

Figure 9: Phase 2 and Phase 3 Mesher Roadmap

Phase 4:

Parents will be using the Mesher application connect with their children's teachers (messages, events, paying for school fees).