



# Fermat

## Welcome to Fermat!

In the last 20 years virtually everything went digital: pictures, music, videos, mails, etc. Nevertheless we still have cash as paper money.

## Why isn't cash money digital yet?

The reason is that digital information can be cloned, and if digital cash could be cloned it would render it useless. When bitcoin was invented it brought with it the solution to the last barrier preventing money to go digital: the solution to the *double spend problem*.

We firmly believe that the next decade will witness governments issuing digital currency based on blockchain technology. We expect paper money is going to disappear within the next 5 to 10 years.

Thus a strong consumer demand for digital wallets will inevitably emerge.

In order to meet this demand thousands of wallets should be available. Wallets will evolve into sophisticated financial applications. Such a wide variety of wallets is indispensable owing to the diversity characterizing the world's population and its financial needs. In fact most of current mobile APPs will turn into financial APPs once we provide them with the ability to easily handle digital cash and digital assets.

## **The Master Plan**

Fermat is a master plan to avoid getting into that future by waiting for independent entrepreneurs to build each of these wallets and financial apps one at the time and from scratch, repeating every time all the math, accounting, cryptography and algorithms that are common to all these APPs. Fermat handles all that and by doing the heavy lifting enables any developer in the world to easily create niche wallets and financial APPs on top of its shared infrastructure.

## **The Framework**

Fermat is a trust-less financial application framework that enables any kind of trust-less applications, including digital wallets.

The framework evolves from the stand-alone crypto wallet and enables an ecosystem of peer-to-peer financial applications that are

both crypto-currency and digital-asset-enabled. The Framework handles a full stack of layers. Starting down from an OS API level, to a Blockchain, Communication, Platform, and User Interface Level.



## The Network

Crypto networks are peer-to-Peer electronic cash systems that allow online payments to be sent directly from one party to another without going through a financial institution. Stand-alone crypto wallets are truth to that principle. But the main benefits are lost if a trusted third party is still required to transport meta-data, synchronize devices, hold wallet files or keys, manage identities, interface crypto networks or the legacy financial system.

Fermat features a peer-to-peer network for transporting meta-data and inter-connect network clients between each other. On top of that network a synchronization scheme transforms a standalone app into

a distributed application across several devices still owned by the same user.



## Fermat Goals

- To allow people with no developing knowledge to build their own desktop and mobile peer-to-peer financial applications in a similar way a non-developer builds a **Wordpress** site: re-using Plug-ins and *themes*.
- To act as a local back-end not only for native-Fermat-APPs and wallets, but also for any other mobile app.
- To be a full-stack Framework in the development of financial applications making them unbannable, reliable and not easy to hack as they are fully decentralized.

# Open Source

The challenge is truly colossal, but we know that the difference between the possible and impossible lies in a team's determination. We have the will to transcend and to spread our vision for this world.

We have the talent, motivation and determination required to create the next generation of financial applications. These will allow people to manage their own digital wallets in a secure way enabling them to interact using their funds in a wide array of transactions and business oriented opportunities across the globe.

We believe the open source community collectively has more influence than any of us individually. Therefore for us it is important to acknowledge and revere services where others invested their time and efforts in order to build. We believe in decentralization.

## Developer Network

We are asking each of you to help lead the way. Because we're already connected with you as we are also developers and designers, and we want to build our relationship with you into a network of developers across the world to share new ideas and forge new collaborations. Working together, we can build the tools and technology that people need to become financially independent, have access from any country to financial products and be safe of nasty third parties spying on them or trying to tell them what they can and can not do with their money. We believe in financial freedom.

We want to hear from you on how we can build this network. We are by now about 35 developers / designers working full time on Fermat and our goal is to reach 300. To learn more about how to join, just read the [how-to-participate-guide](https://github.com/bitDubai/participate-now) (<https://github.com/bitDubai/participate-now>). We hope at every single one of you will join us. Because Fermat and the world need you. We need your skills, imagination and optimism. And with this new network, we're sure we can be partners for decades to come.

We believe in people with passion who are crazy enough to think they can change the world. With a lot of hard work, we believe we can accomplish this.

We won't stop until we do it.

## The Challenge

While designing Fermat we tried to find the answer to the following questions:

- How can we build a P2P network to interconnect all devices between each other in a scalable way?
- How do we get sure the communication is secure?
- How do we build a Plug-ins Framework able to run on smart phones?
- How do we make as much of the code portable to other every OS?
- How do we enable thousands of developers to collaborate?

- How do we make the framework multi-wallet or multi-app?
- How do we let the End User to install more wallets within the same APP and in a P2P way?
- How do we organize Plug-in in order to be reusable by other Plugin?
- How do we prevent a bad Plug-in from stealing the digital funds stored on other Plug-ins?
- How do we make sure information keeps a consistent state even if a phone turns itself off at any time?
- How can we manage multiple identities used by the End User on different wallets / APPs?
- How can we isolate ordinary people from the perceived complexity of crypto currencies?
- How do we integrate merchants, retailers and brands of all sizes in a clever way?
- How can we allow non-developers to create digital wallets without programming anything at all?
- How can we create a fair systems with the developers who contribute to the project?
- How can we use the collective intelligence of the developer community?
- How can we reuse the entire current infrastructure already in place?

The answers to each of these questions are addressed within Fermat.

# What is Fermat?

Fermat is a system where we experiment on what needs to be done for the masses to adopt crypto currencies. As it is very easy to develop mobile APPs on Fermat, entrepreneurs can use it to easily test their business models.

Technically Fermat is an open-source P2P system built on a plug-in architecture that handles a stack of platforms and runs on multiple OS including Android, Linux, iOS, OSX and Windows.

## What makes Fermat different from other wallet systems or services?

- **Fermat is P2P.** This makes it censorship resistant and difficult to hack.
- **Fermat is built with plug-ins.** This enables it to be reused and for any developer to engage.
- **Fermat runs on end users' devices.** This enables users to manage their own money eliminating the need to trust a third party.
- **Fermat is inclusive.** By creating their own plugins, current industry members can integrate with Fermat to offer their services and products to Fermat's already user base.



- **Fermat segments the world population and offers a custom tailored solution for each segment.** Any developer can easily create niche wallets for a particular group of people, for example Brands creating their own wallets for their customers. All the heavy lifting is done by the Fermat underlying technology.
- **Fermat guarantees plugins and wallet developers a revenue stream.** Fermat implements an innovative business model which allows plugins and wallet developers to define a use license, and Fermat itself enforces this license on behalf of developers.

Fermat is moving towards version 1, but we're not stopping there. We have many feature ideas on our [white paper \(FERMAT-WHITE-PAPER.md\)](#) that we're anxious to add. So take Fermat out for a spin and let us know how we can make it your favorite platform to launch your own digital wallet or financial APP.

You can learn more, see some cool images of Fermat's architecture and its P2P network and explore the design space at [Fermat.org](http://www.fermat.org) (<http://www.fermat.org>).

## Fermat's Purpose

- To Empower people with the appropriate tools to save and move their money as a digital format in a more efficient, secure and private way.
- To give back the sovereignty over each one's own resources,

respecting the freedom of choice about which currency to use and how to administrate it, regardless of the place they live or where they were born.

## **Fermat's Mission**

- To get cryptocurrencies mass adopted as soon as possible.
- To build the best possible system able to manage the finances of people.
- To achieve “parity” with the state-of-the-art technology and push towards new frontiers in computer science.

## **Fermat Principles**

### **1. Fermat must not allow censorship.**

- Open Source.
- P2P architecture.

### **2. Fermat must not allow spying on their user base.**

- Point to point encrypted communications.
- Geofenced P2P network enabling the shortest communication path between peers.
- Multi-technology communication layer (cloud, p2p, wifi,

bluetooth, nfc, mesh, etc.).

### **3. Fermat must be secure and resistant to all kind of attacks.**

- No centralized point to be attacked.
- Multiple identities and roles per user.
- Device Private Network (DPN) concept.
- Pocket Money concept and a Multi-Signature Vault owned by the DPN.
- Reviews and Reputation concepts.

### **4. Fermat must never loose a user's funds.**

- Transaction responsibility transmission protocols.
- Remote technical support by wallet and plugins developers.

### **5. Fermat must be useful to each segment of the world population.**

- Niche wallets concept.
- Branded wallets concept.

### **6. Fermat must be extensible and open to innovation.**

- Plugins architecture.
- Multi dimensional layer architecture.

## **7. Fermat must be open and inclusive.**

- Any developer can contribute to the shared infrastructure.
- Any developer can write code for new plugins.
- Any developer can write code for new niche wallets.
- Any developer can fork an existing niche wallet to further specialize it.
- Any graphic / UX designer could provide skins to existing wallets.
- Anyone could provide language packs to existing wallets.

## **8. Each developer must be compensated for their contribution to Fermat.**

- Micro license concept.
- Micro license structure concept.
- Fermat automatically enforcing license agreements.
- Plugin ownership concept.
- Niche wallet ownership concept.
- Branded wallet onwnership concept.
- Master plan design concept, wiht no overlaping functionality but shared ownership.

## **9. Fermat user base must be a shared asset.**

- Any developer must be able to profit from the growing Fermat

user base by writing Plugins this user base could consume via the developers of the wallets they are using.

## **10. Fermat must be inclusive with crypto currency industry members.**

- Any bitcoin | crypto | blockchain established startup could write their own plugins and expose their services to both Fermat developers and the Fermat user base.
- Any alt-coin community could write plugins to enable their crypto currency within the Fermat wallet ecosystem.

## **11. Fermat must be inclusive with the current financial system.**

- Banks and financial institutions could write plugins to enable Fermat wallets to hold funds in banks and other financial institutions.
- Fermat allows its users to move money both from public value transport networks as well as crypto currency networks and also through private or legal financial networks.

## **12. Fermat must be unbanked-people friendly.**

- Multiple logins per device (Device user concept)
- Crypto banking concept.

### **13. Fermat must be OS agnostic.**

- OSA layer concept (Operative System API).
- OS dependent UI on top of Fermat concept.

### **14. Fermat must learn from its user base.**

- Integrated feedback functionality.
- Voting over feature wish-lists concept.

### **15. Fermat must be the financially most efficient way to move or spend the end user's money.**

- Crypto Vault for multiple wallets concept.
- Financial AI Agents concept.

### **16. Fermat must facilitate the regional distribution and access to crypto currencies.**

- Crypto Distribution Network concept.
- Crypto Brokers concept.

## **How to Install and Run Fermat**

### **Download**

Installers for the latest version of Android can be [downloaded here](http://fermat.org/fermat.apk) (<http://fermat.org/fermat.apk>). Mac, Windows and Linux (Debian/Ubuntu) will be supported in the near future.

## Installation

In addition to the core features built into Fermat, there is a growing community of developers building *Plug-ins* and *Niche Wallets* that add all sorts of useful functionality.

For instructions on how to install and run the source code, see the [Installation Guide](https://github.com/bitDubai/fermat/blob/master/README-INSTALLATION.md) (<https://github.com/bitDubai/fermat/blob/master/README-INSTALLATION.md>).

## Need Help?

Having problems compiling or running Fermat the first time, or not sure how to use Fermat? Please log into the [IRC DEV Channel](http://irc.lc/freenode/fermat-dev/) (<http://irc.lc/freenode/fermat-dev/>), and we will help you to fix common problems and find extra help if needed.

## Learn More?

Take a look at the [Fermat Book](https://github.com/bitDubai/fermat/tree/master/fermat-book) (<https://github.com/bitDubai/fermat/tree/master/fermat-book>) that it is being written in order to help developers learn more about Fermat

technology.

## Project status

As of November 2015 the project status is the following:

**Code state** : Under development for 6 months. No releases yet. Many full time developers working on it provided by the project's main contributor: [bitDubai \(https://www.bitDubai.com\)](https://www.bitDubai.com).

**Future path of development** : Active (First release with very limited features scheduled for December 2015).

## I Want to Join the Team!

Awesome!

*There are lots of ways you can help.*

## Developers

If you are a developer and want to contribute from a bug-fix up to building a whole financial APP on top of Fermat, please read the [Contributing Guide](https://github.com/bitDubai/fermat/blob/master/CONTRIBUTING.md) (<https://github.com/bitDubai/fermat/blob/master/CONTRIBUTING.md>), then learn how to pull the repo and hack on Fermat. Then say hi at our [IRC DEV Channel \(http://irc.lc/freenode/fermat-dev/\)](http://irc.lc/freenode/fermat-dev/) or you can



also find us on [Facebook \(https://www.facebook.com/FermatOrg/\)](https://www.facebook.com/FermatOrg/).

## Others

You don't need to be a developer to participate on the project. There are many ways to do it and we explain each one of them at the [How to Participate Guide \(https://github.com/bitDubai/participate-now\)](https://github.com/bitDubai/participate-now).

