**MVP:**

1. **Ordering hardware:**
   1. **SIM Overlays**
      1. **Emailed** [**Taisys**](https://www.taisys.com/index) **for 2-5 samples Jan 3**
         1. **Responded asking for more info on my app and hasn’t responded since**
      2. **Ordered 5 samples from (**[**Alibaba**](https://biz.alibaba.com/contract/draftSampleOrder.htm?KEY=a1e868cccc976166481dd2dd024d46bf#/) **$30 USD), shipped on jan 9**
   2. **PCSC reader**
      1. **Ordering from amazon (**[**SRC-3500 A**](https://www.amazon.ca/Identiv-SCR3500-Smartfold-Smart-Reader/dp/B0040671WU/ref=pb_allspark_purchase_sims_desktop_2/142-5646745-1356411?pd_rd_w=JHJ0T&pf_rd_p=9bc53186-2058-4537-b002-f31a0b7a2266&pf_rd_r=M46TC5GDAYJSSHZR8TRV&pd_rd_r=85ccf228-80fc-41bc-8023-ccf261e6add2&pd_rd_wg=jj6Vf&pd_rd_i=B0040671WU&psc=1)**, $17) on Jan 10**
2. **Decide on basic MVP features:**
   1. **Offline payment**
   2. **Online payment without relayer (internet required)**
   3. **Online payment with relayer (no internet required)**
   4. **Every thinSIM can be a relayer**
3. **Wireframe backend logic on XD, based off** [**thinSIM research**](https://kurti.sh/pubs/thinsim-based-attacks.pdf)
4. **Create prototype of front-end UI on adobeXD, based off** [**DigiTally**](https://kbaqer.com/papers/DigiTally_SOUPS2017.pdf)
5. **List each feature, assign deadlines**
6. **Code java applet, run on java sim card simulator**
7. **Upload applets to sim card overlays using PCSC reader and** [**android SEEK**](https://seek-for-android.github.io/)**, test a transaction on two old phones**
   1. **Need to get a nokia…**
8. **Show the prototype to Leon, apply for CDL or gitcoin funding/public goods funding/other blockchain funding or bill and melinda gates/UN SDG funding or all the above**

**SIM Research Plan: (easy, medium, hard) (watch** [**this**](https://www.youtube.com/watch?v=31D94QOo2gY&t=3s)**, then look at** [**this**](https://simhacks.github.io/) **and use these** [**docs**](https://docs.oracle.com/en/java/javacard/3.1/guide/install-and-setup-development-kit.html) **to set up development environment on eclipse)**

1. **Determine memory, storage, and compute capability range for sim cards** [**(useful)**](https://www.hmoob.in/wiki/SIM_card)
2. **Write Java applet “front-end” with basic wallet functions**
   1. **Order 2 sim Overlays, use GlobalPlatform to load “hello-world” on them and conduct a transaction**
3. **Write Java applet “back-end”**
4. **Determine how to use sim secret to sign an sms message**
5. **Determine how to encrypt sms messages**
6. **Determine how to asynchronously update state (watch** [**this**](https://www.youtube.com/watch?v=IbfG_KSlTD4)**, read** [**this**](https://www.cl.cam.ac.uk/~rja14/Papers/SPW24.pdf)**, skim** [**this**](https://www.cl.cam.ac.uk/~rja14/Papers/DigiTally_SOUPS2017.pdf) **and** [**this**](https://www.repository.cam.ac.uk/bitstream/handle/1810/285001/kabhb2-thesis.pdf?sequence=1&isAllowed=y)**)**
   1. **Delay-tolerant network, store-and-forward mechanism**
   2. **Should state be kept “local” until a user with internet ‘syncs’ (least hassle, what about price fluctuations for non-stablecoins)**
   3. **Should a copy of every txn be sent to a number which is set up to update the state (1 extra message sent from the user, need to have new numbers that aren’t taken down by telcos)**
7. **Determine how to onboard users**
   1. **Go to someone with internet, who downloads it for you?**
   2. **Possible to update over-the-air? If we can, can’t the carrier censor and control as well?**
   3. **Get it in an sms from someone, it downloads for you? Susceptible to hacks or phishing?**
   4. **Get it on a SIM overlay (poor) or eSim (rich)**
8. **Determine how to make ramping easier, decentralized for hawala traders and anyone interested**
9. **Determine how to transfer assets if sim card is lost, if switching to a new sim card**
10. **Determine business model:**
    1. [**If anyone seeking to monetise a break of a card needed, as a practical matter, to extract money from merchants (as the other users are too dispersed and too poor) then it could make perfect business sense.**](https://www.cl.cam.ac.uk/~rja14/Papers/SPW24.pdf)
    2. **Two-pronged approach? eSIM applet wallet with DeFi (we earn % of their yield in exchange for portfolio management) and NFC payment capability for premium users (** [**255 M phones 2020 to 721 M in 2025**](https://www.statista.com/statistics/1027280/global-esim-device-shipments/)**), eSim is a growing nascent market, should grow along with crypto adoption. This subsidizes ThinSims for the poorest/everyone else**
    3. [**iSims (system-on-chip) coming out, top security**](https://developer.qualcomm.com/blog/rise-esims-and-isims-and-their-impact-iot)
11. **Meet key people:** 
    1. **Ross Anderson (cryptoeconomics expert, DigiTally), Khaled Baqer (delay-tolerant networks DigiTally), Nafay Chaudry (hawala Afg), Leon Vandenberg (Fuzo, Creative Destruction Labs advisor and waterloo prof), Dave Dobbin (former Roamly CEO, SIM overlay in Rhill, went to York), Fereshteh Forough (Code to inspire Afg, cash transfers through crypto during Talib takeover), Rowan Phipps (SIM overlay hacking research)**

**1. Determine memory, storage, and compute capability range for sim cards**

[**SIM application toolkit spec**](https://www.etsi.org/deliver/etsi_ts/101200_101299/101267/08.18.00_60/ts_101267v081800p.pdf)

[**Smart Cards; UICC Application Programming Interface (UICC API) for Java Card™**](https://www.etsi.org/deliver/etsi_ts/102200_102299/102241/13.00.00_60/ts_102241v130000p.pdf)

[**Specification of the Subscriber Identity Module - Mobile Equipment (SIM - ME) interface; (GSM 11.11)**](https://www.etsi.org/deliver/etsi_gts/11/1111/05.03.00_60/gsmts_1111v050300p.pdf)

**Main types of Sim cards:**

| **SIM card format** | **Introduced** | **Standard reference** |
| --- | --- | --- |
| **Full-size (1FF)** | **1991** | [**ISO/IEC 7810**](https://en.wikipedia.org/wiki/ISO/IEC_7810)**:2003, ID-1** |
| **Mini-SIM (2FF)** | **1996** | **ISO/IEC 7810:2003, ID-000** |
| **Micro-SIM (3FF)** | **2003** | [**ETSI**](https://en.wikipedia.org/wiki/ETSI) **TS 102 221 V9.0.0, Mini-UICC** |
| **Nano-SIM (4FF)** | **early 2012** | **ETSI TS 102 221 V11.0.0** |
| **Embedded-SIM**  **(eSIM)** | **2016** | **ETSI TS 102.671 V9.0.0**  [**JEDEC**](https://en.wikipedia.org/wiki/JEDEC) **Design Guide 4.8, SON-8**  **GSMA SGP.22 V1.0** |

**All versions of the non-embedded SIM cards share the same** [**ISO/IEC 7816**](https://en.wikipedia.org/wiki/ISO/IEC_7816#7816-2) **pin arrangement.**

**Sim overlays:**

**o** Thin strips that connect to sim cards, allow for programmability on top of sim cards

o Implemented by [Equity Bank](https://mobitrends.co.ke/equity-bank-thin-sim-technology/#:~:text=The%20Thin%20SIM%20is%20an,as%20well%20as%20feature%20phones.) in Kenya now, what Fuzo tried to do, [JCI and Taisys doing it for crypto cold wallets in China](https://www.telecompaper.com/news/jci-taisys-to-deliver-cryptocurrency-cold-wallet-in-sim-overlay--1289946), Roamly (canadian based, CEO Dave Dobbins tried to market it to business-class fliers, flopped)

* [Malicious code on thin sim can do bad stuff without user knowing](https://kurti.sh/pubs/thinsim-based-attacks.pdf) 
  + But ways to prevent it (sandbox thin SIMs, see what JCI and Taisys in Japan, and Taisys and Eroute in India are doing)

**Known security threats:**

1. [Simjacker](https://en.wikipedia.org/wiki/Simjacker) with S@T browser, WIB
2. [SIM cards that use DES (Data Encryption Standard)](https://srlabs.de/rooting-sim-cards/)
3. For SIM overlay, threat of Man in the middle attacks and interference with other sim card applets and comms with the network, can be mitigated if sandboxed, as in the example of DigiTally ([Note that the overlay SIM (and the DigiTally applet) does not compromise users’ privacy in our implementation, since it operates as an independent sandboxed applet and does not interfere with other applets’ data if there are any installed)](https://www.cl.cam.ac.uk/~rja14/Papers/DigiTally_SOUPS2017.pdf)
   1. In response to rainbow table attacks of sim cards OTA where error messages are signed, we can limit number of errors? DigiTally made sure each SIM was programmed to lock itself after a certain number of failed attempts to access the contents of the trusted tamper-proof environment.
   2. Money tracking: Participants liked being able to review their last transaction and balance. For some, however, this was not enough. It was suggested that this feature would be more useful if the user could review all previous transactions.
   3. Our prototype error-recovery mechanism needs a redesign. A simple alternative would be a menu option to reset transaction data, requiring authentication with the user’s PIN rather than requiring them to enter dummy inputs.

**Storage:**

· 8kb up to 256 kb

**What is stored:**

**·**  Unique serial number (ICCID), international mobile subscriber identity (IMSI) number, security authentication and ciphering information, temporary information related to the local network, a list of the services the user has access to, and two passwords: a personal identification number (PIN) for ordinary use, and a personal unblocking key (PUK) for PIN unlocking. In Europe, the serial SIM number (SSN) is also sometimes accompanied by an international article number (IAN) or a European article number (EAN) required when registering online for the subscription of a prepaid card.

**Crypto for fragile states**

* **Problem**: US froze Afghan central bank assets. Economic freefall, middle-class into poverty, loss in central bank confidence. US has no incentive to eliminate sanctions long-term (i.e. Iran) and even if they did, the Taliban (repressive regime) would gain significant legitimacy. Humanitarian assistance cannot replace economy med/long-term.
* **Question**: Can access to crypto circumvent both the US government and to some degree, the Taliban, while restoring and enhancing economic inclusion for the average Afghan with a mobile phone?
* **Threats**: [Retaliation from US](https://www.wsj.com/articles/growing-use-of-cryptocurrency-in-afghanistan-poses-security-concerns-11631275200) (worries about sanction circumvention and terrorist financing), [retaliation from Taliban](https://www.bbc.com/news/business-59129470) (already banned foreign currencies)
* **Challenges**: [Existing financial exclusion](https://blogs.worldbank.org/endpovertyinsouthasia/pathway-financial-inclusion-afghanistan) (85% of Afghanistan unbanked), [low literacy rate](https://uil.unesco.org/interview-literacy-rate-afghanistan-increased-43-cent) (43% total pop’n, however youth aged 15-24 is 65%, large discrepancy between men 55% and women 30%), innumeracy rate (cant find stats), [low internet penetration](https://www.dw.com/en/will-the-taliban-restrict-internet-access-in-afghanistan/a-59029364) 13.5%, poverty and metered prepaid accounts.
* **Opportunities:** High mobile subscription rate (22 million phones registered, 58 per 100 people), Examples of crypto use among Afghans ([Code To Inspire](https://unchainedpodcast.com/crypto-actually-fixes-this-how-code-to-inspire-uses-crypto-in-afghanistan/) Fereshteh Forough sending cash assistance to students using crypto, [Roya Mahboob](https://www.reuters.com/article/crypto-currency-afghanistan-idUSL8N2QU39A), [others](https://www.cnbc.com/2021/08/21/bitcoin-afghanistan-cryptocurrency-taliban-capital-flight.html))
* **Other players**: Afpay (central bank e-payment solution) was about to be implemented in August just before the regime collapsed, Mobile Network Operators had their own mobile money systems (i.e. Roshan), hawala system for “transferring money without moving it” is a long-established system and could be an intermediate step for on-boarding and a more permanent on/off ramp to fiat with incentives for participation (fees)
* **Missing infrastructure**: Accessing blockchain from dumbphones.
* **Benefits:** lower fees, faster transfers, would unlock access to crypto not just for Afghans, but for all those in the world with dumbphones (billions of people), undermine predatory mobile money operators with high fees, significantly reduce remittance fees and wait-times, undermine sanctions regimes
* **Pathways**:
  1. Internet (more secure and fastest to implement, less equitable as only 13.5% of population could access for now, more convenient for users, more under the radar to avoid retaliation)
  2. Sms (less secure as sms is known to be interceptable where 2G security < 3G security < 4G security and in afghanistan there are [2.8 M 2G users, 2.9 M 3G users, and 1.4 M 4G users](https://atra.gov.af/#/); more equitable as *up to but very likely less than* 58% of the population would have access, more convenient as sms is very accessible)
  3. SIM Application Toolkit (more secure, more inconvenient as users have to get a new or updated sim card OR use [S@T Browser like simJacker](https://www.makeuseof.com/tag/ways-sim-card-hacked/) and [WIB](https://www.andreafortuna.org/2019/09/28/wibattack-not-only-s-t-browser-but-also-wib-sim-toolkit-is-vulnerable-to-simjacker-attacks/))
     1. To exploit simJacker pathway, send an sms, user clicks on the link in the sms, content can be downloaded on phone’s SIM card/sensitive functions can be performed, location data can be retrieved…
     2. SIM cards have 1mb of data, private key stored in 8 bytes, can also store contact info. Some phones have private key stored in phone’s memory instead.
     3. Can carriers steal data on the SIM?
  4. USSD (more secure, more convenient, code allocation controlled by network operators who often demand a ~50% cut)
     1. [Mobile money systems built on USSD use a similar set of menus as STK applications. However, with USSD each message travels to the server rather than just to the SIM. As there is no logic on the phone for anything except presentation of the messages, the responses to menu items are sent unencrypted to the server, relying on GSM encryption to provide security.](https://kurti.sh/pubs/thinsim-based-attacks.pdf)
* **Questions**:
  + Does anything like this exist?
  + Examples that use sms for payment but not crypto
    - mPaisa (safariCom) and mhawala