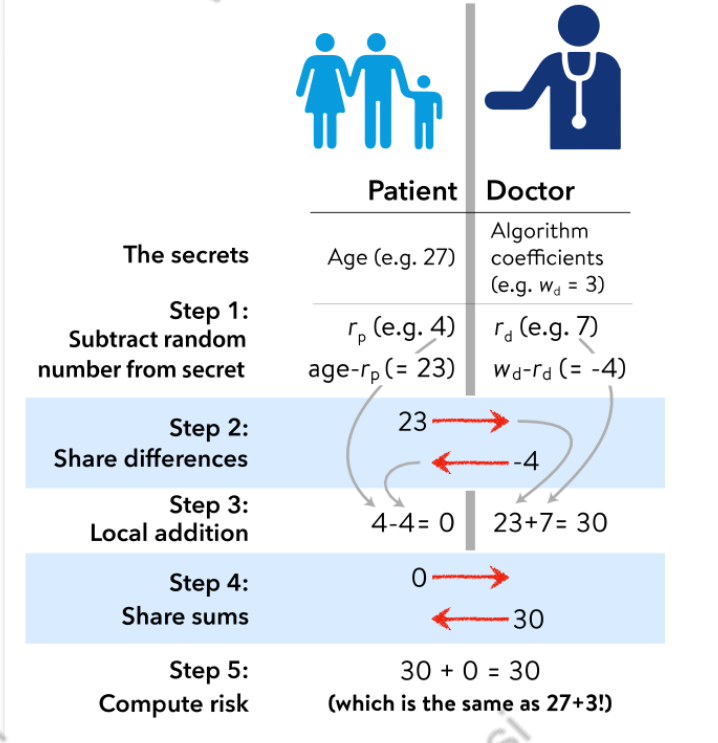
***Mi smo Enya***
*Začeli smo v Palo Alto v Kaliforniji, ki razvija varnostne in zasebne tehnologije za zaščito potrošnikov in bolnikov.*

***Kakovost podatkov***
*Zemljevid prikazuje podatke o množici ljudi, ki so jih delili ljudje okoli vas. Ker gre za zemljevid množice, morda ni natančen. Vendar pa večina ljudi, če jim je omogočeno anonimno posredovanje podatkov, ponavadi natančno poroča, zlasti v situacijah, v katerih je to koristno za njih in njihovo skupnost.*

***Kako uravnotežimo vpogled in zasebnost?***
*Tradicionalno biomedicinske raziskave (in zdravstveno varstvo) vključujejo prenos občutljivih podatkov (kot so vaše ime in zdravstveni simptomi) medicinskim strokovnjakom in znanstvenikom. Vendar lahko v računalniške sisteme vdrejo ali zlomijo in zanimivo je razmišljati o načinih, kako bolje zaščititi svojo zasebnost in podatke, hkrati pa zdravnikom in javnim uslužbencem omogočiti, da dobijo informacije, ki jih potrebujejo za sprejemanje najboljših odločitev. Na srečo nova računalniška in kriptografska orodja omogočajo uravnoteženje vpogleda z zasebnostjo. Pri FeverIQ uporabljamo "varno računanje več strank".*

***Kako to deluje? Varno računanje več strank (SMC)***
*Predstavljajte si, da ste zdravnik, ki preučuje SARS-nCoV-2. Ena prvih stvari, ki bi jih morda želeli vedeti, je, koliko so stari ljudje s pozitivnim testom SARS-nCoV-2. Da bi dobili te informacije, lahko poskusite vprašati več milijonov ljudi za njihov datum rojstva, vendar večina ljudi raje ne pove. Med drugimi banke uporabljajo te podatke za preverjanje identitete osebe.* ***Bi dali datum svojega rojstva nekomu, ki vas je samo kontaktiral po e-pošti? (Upajmo, da ne!)***

*Tu je še en način - zdravnik bi lahko prosil vse, naj v svojo starost dodajo naključno število med -100 in +100 in predloži rezultat. Če je torej vaša starost 27, vaša izbira naključnega števila pa -12, bi odšteli 12 od 27 in rezultat, 15, poslali zdravniku. Zdravnik potem ne bi vedel vaše starosti, vendar lahko še vedno ugotovi nekaj zelo koristnega, to je porazdelitev starosti ljudi s pozitivnim rezultatom testa SARS-nCov-2. Da bi to naredili, bi zdravnik povprečno ocenil veliko odzivov. Podobno kot je nični povprečni premik razpršenega koščka prahu, se naključni izrazi navadno odpovejo, postopoma razkrivajo dobro oceno resnične starostne strukture prebivalstva.*
*Ta pristop deluje dobro za raziskave, vendar obstaja očitna težava - v značilnem medicinskem kontekstu pacient pričakuje, da jim bo zdravnik povedal nekaj o svojem zdravju in ne samo dajal abstraktne izjave o demografskih podatkih svetovne dobe. K zgornjemu pristopu dodamo nekaj računskih zasukov. Tu je poenostavljen primer varnega računanja več strank.*




*Predstavljajte si, da je zdravnik razvil nov algoritem za oceno tveganja za okužbo. Recimo, da gre za preprost dodatek, kot je tveganje = starost + 3. Pacientka, Alice, bo morda želela ohraniti svojo skrivnost (= 27) in zdravnik bo morda želel zaščititi njen algoritem (tveganje = starost + 3). Kot je prikazano na sliki, bi se lahko obe strani strinjali z naslednjim. Najprej bi lahko oba odšteli naključno število od svoje skrivnosti (korak 1) in nato delili razlike (korak 2). Nato lahko vsak doda svoje naključno število v delež druge stranke (korak 3) in nato izmenja rezultate teh izračunov (korak 4). Končno bi lahko ena (ali obe) stranki dodali deleže in razkrili bolnikovo tveganje (= 30), ne da bi v vsakem trenutku prenesli bodisi bolnikovo starost bodisi zdravnikovo skrivnost.*

***Kako to deluje matematično?***

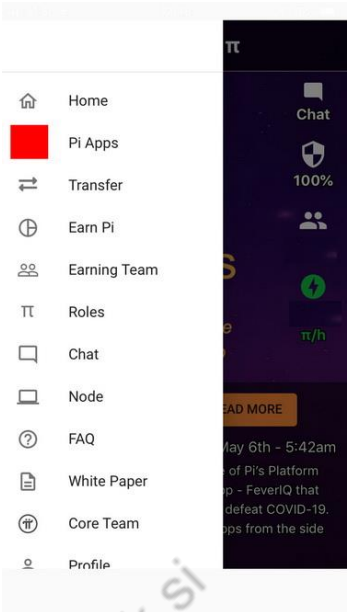
*Če ste spremljali vse izraze, vidite tveganje = (starost - rp) + rd + (wd - rd) + rp = starost + (rp - rp) + (rd - rd). Srednja dva izraza ocenjujeta na nič, poenostavitev izraza do želenega rezultata, tveganje = starost + wd. V bistvu obe strani vbrizgata hrup v komunikacijski protokol, hrupni signal opravi predhodno dogovorjene linearne matematične operacije, nato pa se hrup odpravi na samem koncu. Dejstvo, da se obe strani spominjata in ne razkrivata oziroma ne delita svojih pogojev hrupa (rp oziroma rd), je tisto, kar ščiti skrivnosti.*
*Ta poenostavljeni primer izpušča podrobnosti, potrebne za to, da takšni sistemi delujejo v praksi - najbolj očitno je, da lahko v tej shemi igrač pacient takoj pridobi skrivnost zdravnika, wd, tako da obrne algoritem (tveganje - 27 = 3). Takoj, ko se skrivnosti na obeh straneh zapletejo, postane izredno težko, če se bosta obe strani naučili (ali celo ocenili) skrivnosti druge strani. Množenje zahteva dodatne korake, na primer matematično seznanjene naključne številke, imenovane Beaver Triples.* ***Če ste prebrali do te točke, vas bo morda zanimalo več - tukaj je izvirna publikacija o Beaver Triples iz leta 1991 (Učinkoviti***

***večstranski protokoli z randomizacijo vezja).***
*V podjetju Enya delamo na orodjih za gradnjo takšnih aplikacij, ki ohranjajo zasebnost. Če želite izvedeti več, si oglejte naš SDK.*

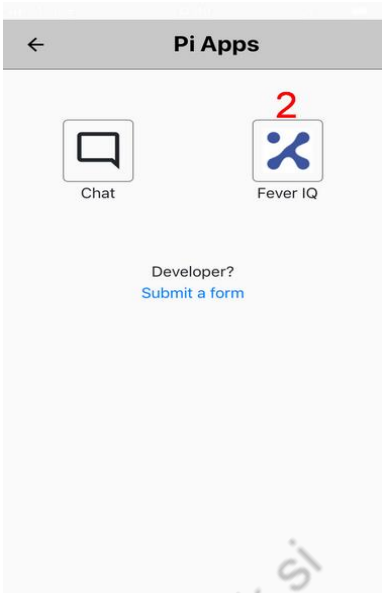
***Pod pokrovom - kako varno raziskujemo nove simptome COVID?***

*Naš prvi korak je ustvarjanje kandidatov za prenašalce simptomov z upoštevanjem biomedicinske literature, nacionalnih in mednarodnih zdravstvenih organizacij, kot so CDC in WHO, poročila o primerih zdravnikov in družbeni mediji. Na primer, kandidatski vektor za navadni prehlad je lahko {kihanje, izcedek iz nosu}, medtem ko je lahko vektor simptomov za COVID {vročina, modri prsti, izguba vonja}. Ko nekdo prispeva svoje simptome v FeverIQ, se prva stvar zgodi, da so njihove skrivnosti (npr. Vročina === resnična) zaščitene z uporabo SMC. Z uporabo SMC nato izračunamo njihovo matematično (Hamming) razdaljo do (trenutno) štirih različnih vnaprej konfiguriranih vektorjev simptomov, ki predstavljajo "prehlad", "gripo", "COVID-basic" in "COVID-nevro". Ko se izračuna zaključi, nam ostane šest številk - približno mesto osebe (npr. "Palo Alto" ali "Hong Kong"), njihova matematična bližina štirih predhodno konfiguriranih konstelacij simptomov in število, ki predstavlja {"no test", " negativni test "," pozitiven test "}. S temi informacijami lahko pomagamo drugim, da raziščejo, v kolikšni meri različna konstelacija simptomov napoveduje negativen ali pozitiven rezultat testa in tudi količinsko ugotovijo, ali lahko različna konstelacija simptomov razlikuje med različnimi boleznimi (npr. "Gripa" v primerjavi z "COVID" ).* ***Ena od pričakovanih dolgoročnih koristi pri zbiranju teh informacij je, da bodo uradniki v javnem zdravstvu lahko bolje razdelili omejene vire za testiranje.***

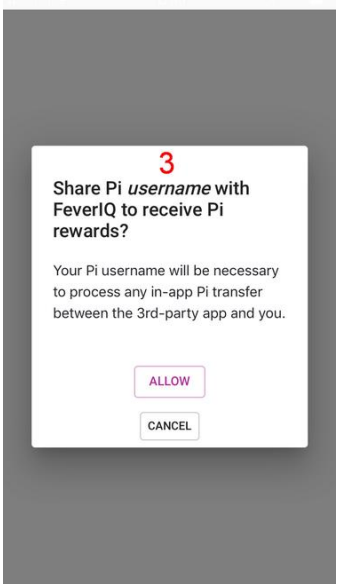
***1.Dostop do aplikacije***



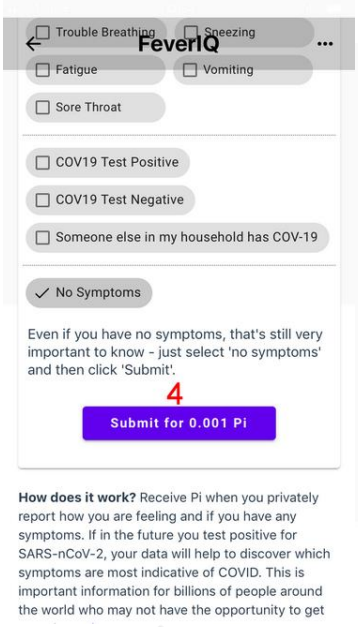

***2. Klik na Fever IQ***



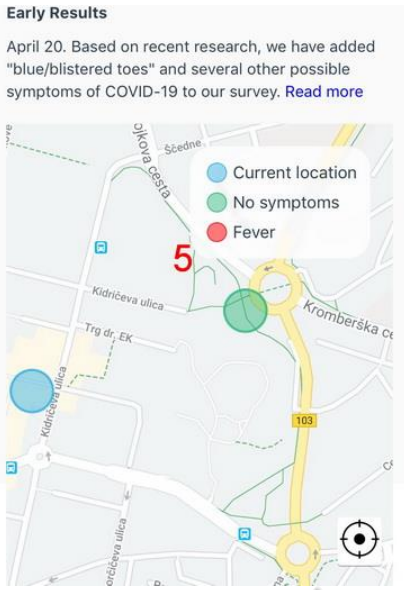

***3. Odpre za potrditev user name v aplikaciji (nakazilo za sodelovanje)***



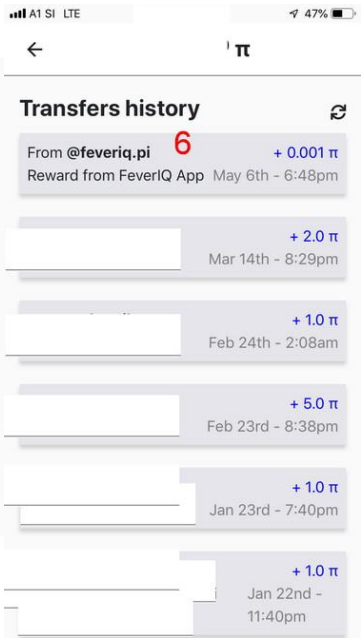
***4. Anketa in plačilo Za vaše sodelovanje***




***5.Zelen krogec v app, daleč od dejanske lokacije, varovanje zasebnosti***




***6. Nakazilo za vaše sodelovanje***



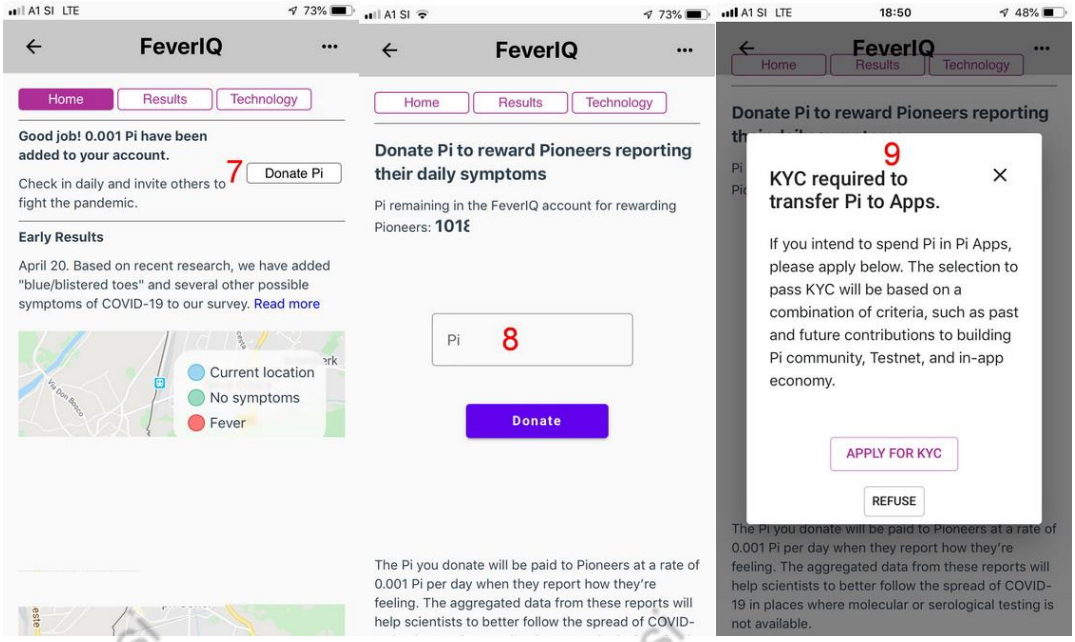

***Na spodnjih slikah pa sedaj sledijo postopki, kateri so za skupnost najbolj zanimivi!***

***Nakazilo ste dobili. Ali ste pripravljeni tudi kaj donirat ? Če ste se, se vam bodo odprli naslednji koraki….. KYC, anketa kaj ste naredili oz. kaj boste naredili za skupnost…..***

***7.Donacija***

***8.Izberete znesek donacije v Pi***

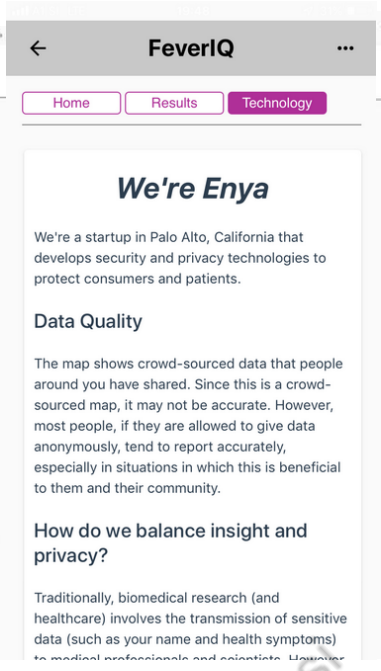
***9. Po donaciji vam odpre za KYC***

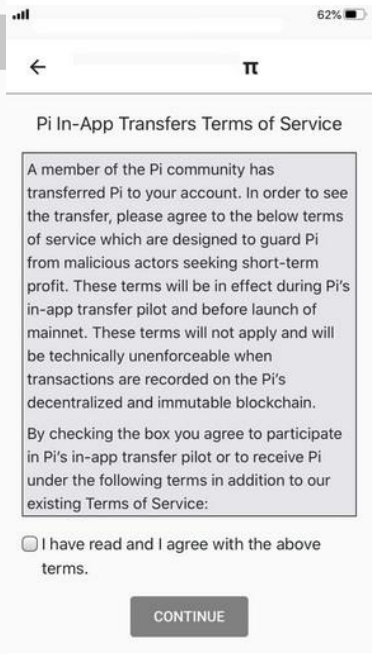


***10. Anketa – kaj ste in kaj boste naredili za skupnost***

***11. Lahko si tudi malo pogledate po app FeverIQ***

***Potrditi boste morali tudi da prejmete nakazilo***


***Srečno Pionirji in veselimo se vašega sodelovanja…..***

***Ekipa Pi Slovenije, vedno z Vami.***