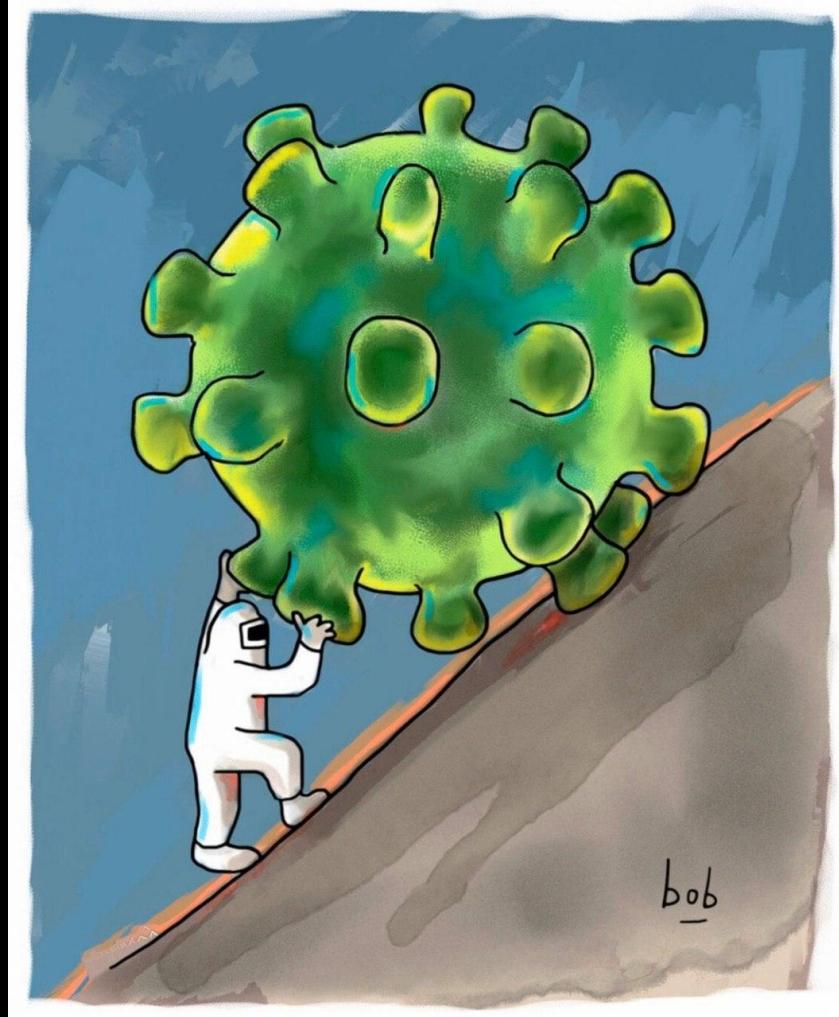




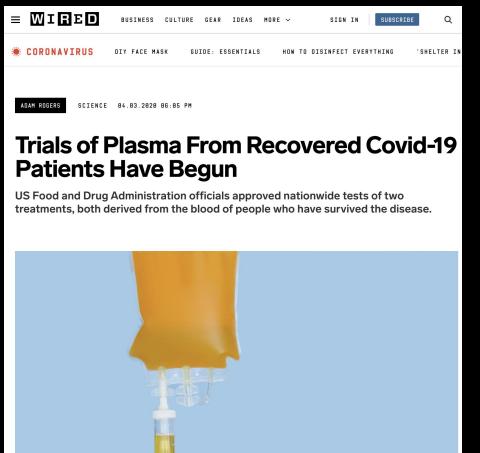
dPlasma

Data is the medicine we need

1.The Problem



Clinical Trials of Convalescent Plasma



An official website of the United States government [Here's how you know](#)

BLOOD FROM COVID-19 SURVIVORS: THE WAY TO A CURE

A 100-year-old way to beat disease could help researchers the antibodies from earlier patients to help the newly infected.

LETTERS TO HEALTH CARE PROVIDERS

IMPORTANT INFORMATION ON THE USE OF SEROLOGICAL (ANTIBODY) TESTS FOR COVID-19 - LETTER TO HEALTH CARE PROVIDERS

The U.S. Food and Drug Administration (FDA) recommends that health care providers continue to use serological tests intended to detect antibodies to SARS-CoV-2 to help identify people who may have been exposed to the SARS-CoV-2 virus or have recovered from the COVID-19 infection. Health care providers should also be aware of the limitations of these tests and the risks to patients and the community if the test results are used as the sole basis to diagnose COVID-19.

The FDA is not aware of an antibody test that has been validated for diagnosis of SARS-CoV-2 infection. While the FDA remains open to receiving submissions for these tests for such uses, based on the underlying scientific principles of antibody tests, the FDA does not expect that an antibody test can be shown to definitively diagnose or exclude SARS-CoV-2 infection.

RECOMMENDATIONS

The FDA recommends health care providers:

- Continue to use serological (antibody) tests, as appropriate, and be aware of their limitations.
- Do not use serological (antibody) tests as the sole basis to diagnose COVID-19 but instead as information about whether a person may have been exposed.



Treatment of Patients with COVID-19 Convalescent Plasma (CCP)

Rita Reik, M.D.
Chief Medical Officer

Martin Grable
EVP Corporate Development

Richard R. Gammon, M.D.
Medical Director

Florida Society of Pathologists
April 5, 2020

It's happening!

Donors in Florida

COVID-19 Convalescent Plasma Donor Eligibility

- You must be eligible to donate blood
- You must have a prior diagnosis of COVID-19 documented by a laboratory test
- You must have fully recovered from COVID-19 with complete resolution of symptoms for at least 14 days before donating plasma for this purpose
- Have a negative result for COVID-19

If you think that you are qualified and are willing to help, or if you have questions about being a COVID-19 convalescent plasma donor, please contact OneBlood at 1-888-9Donate (1-888-936-6283), and select option 9, or talk with your physician.

2.The Solution

What is that we are building? And why now?

App for matching plasma donors to patients in the CPP (Convalescent Plasma Program) requirements in any country of the planet.

(This is not for everybody yet, but the studies are promising!)

Quick, reliable & privacy-preserving matching mechanism globally that is easy to use.

COMPATIBILITY MATTERS

COORDINATION MATTERS (Supply chain Infrastructure)

JURISDICTION MATTERS (Today)

tinder

It's a Match!



 Send Message

 Keep Swiping

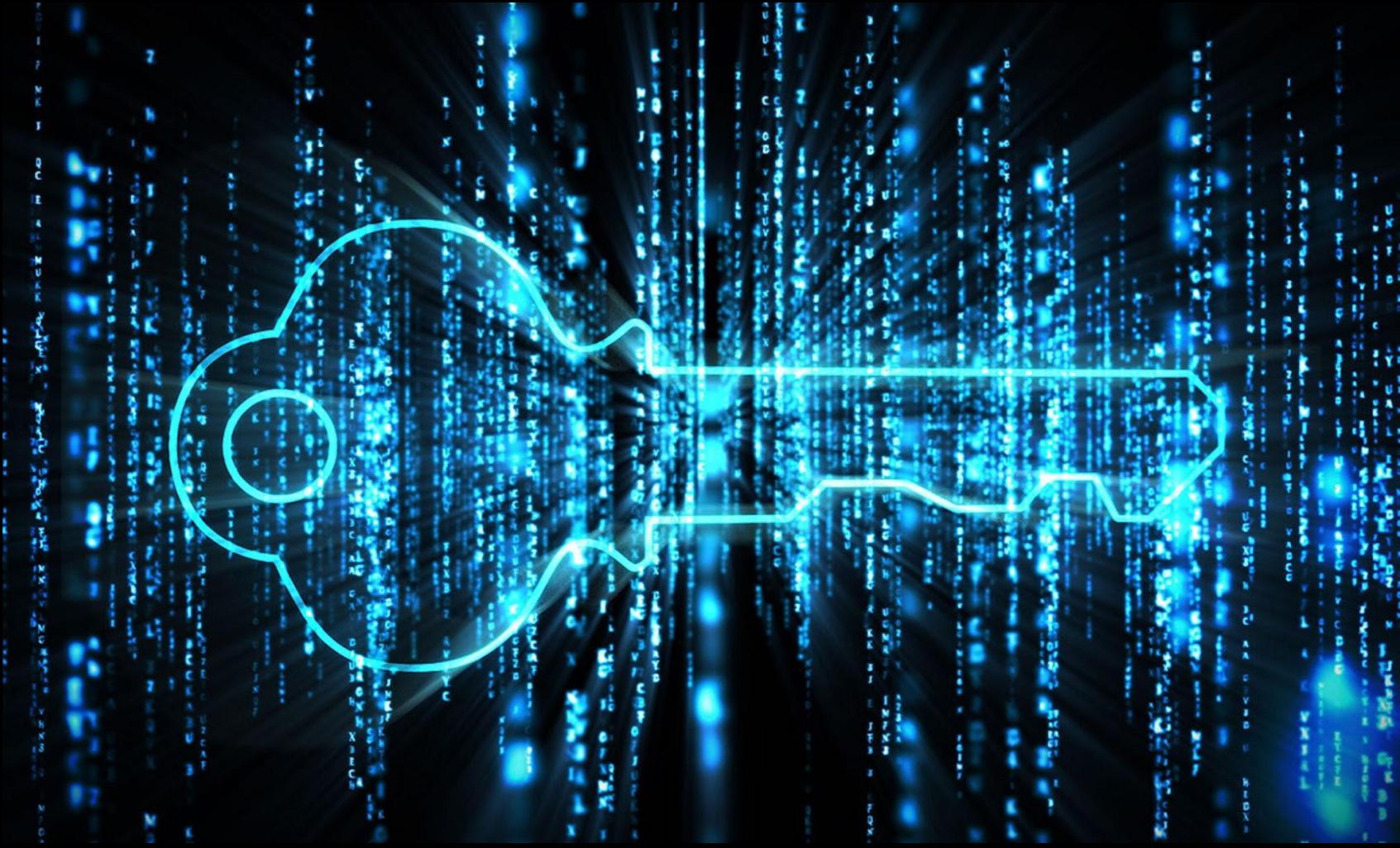


Emily & James 4/30/2016

3. Do we need the Blockchain?

F045C3AC4A21BE 87FD 52 00 573B15200000 2
325E3FDDA85BECCB9FE1 180 00 47748767BAD898
B 66C8D4CAA05F28B 6386C 00 8923589A 3
1704F0722924768 00 38151
7 19A5C77B 25BE70 A1C 00 1FO 2707
9B038B7C3D15 00 CABA2
38EEE6B4925926B22 B31DE24
36E5B4A2 5 83C64064F
8 F39A7B5 AC44A468490
9 56792B5095BFBC56059
C1179CE73532277B13 00
8D12B8AAA7F8F089 00
B0 A2A0E3C26C4E904 00
F045C3AC4A21BE4E7FD052
8325F3 A85BECCB9FE1 00
6 C8D CAA05F28B26386C42CC 00
0 07229247687363 00
19AA5C77BC2 00
8B7C33 00





4. Competitors

Amazon lends its expertise — and its cash — to Covid-19 research

By ERIN BRODWIN @erbrod / MAY 7, 2020



"I've been very impressed with their level of commitment," Lipkin told STAT.

Connecting potential plasma donors and researchers

Amazon Web Services, the company's web services provider, has pitched in to help build an online registry for potential plasma donors. The site, created in collaboration with Michigan State University, lets potential donors sign up to be contacted by local researchers. So far, the site enrolled 10,000 potential donors, an Amazon spokesperson said.

Nigel Paneth, a professor of epidemiology at Michigan State and the lead on the website, said AWS contacted him out of the blue one day to ask if they could help.

Related: Will employers still shell out for health tech benefits in an unemployment crisis? The industry is about to find out

Paneth and his colleagues now meet weekly with several AWS staff members to troubleshoot problems and talk about the website's latest needs. They're also working on developing a donor-matching program that would allow donors to connect with researchers accepting donations in their area.

The website also has resources for clinicians on the ongoing research of blood plasma for Covid-19. It lets clinicians record notes on how patients who've received plasma for Covid-19 outside of a clinical trial are responding to the treatment and also lists FDA-approved clinical trials of plasma. The researchers hope the responses offer an early look at how plasma is affecting patients while they await the results from clinical trials.

"Hopefully we can start to see a little bit of a signal before the results from the randomized controlled trials come in," Paneth said. "No one knows whether this is going to work."

Studying the spread of Covid-19

Amazon is also funding a study by the Fred Hutchinson Cancer Research Center, based in Seattle, that aims to collect data on Covid-19's infection rate, how long an

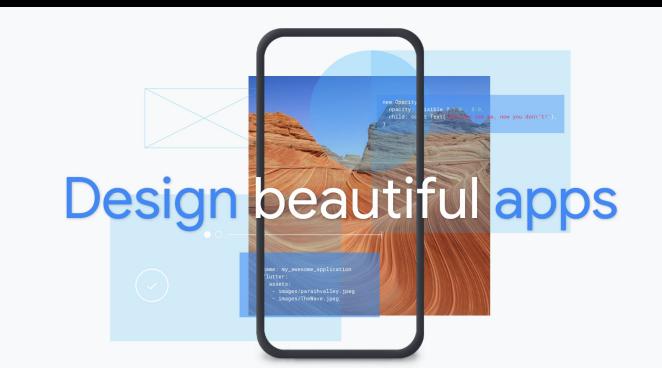
605 Bn

Facebook's Market Cap

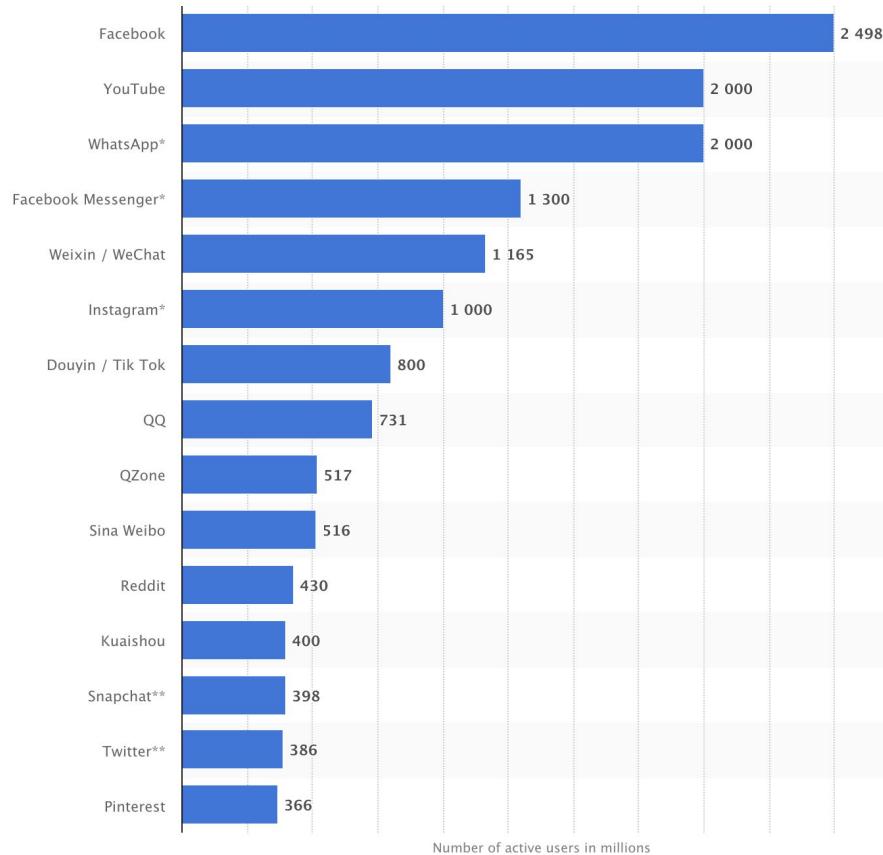
3.2Bn

number of devices reach

In April 2020, over 98 percent of facebook's active user accounts worldwide accessed the social network via any kind of mobile phone.

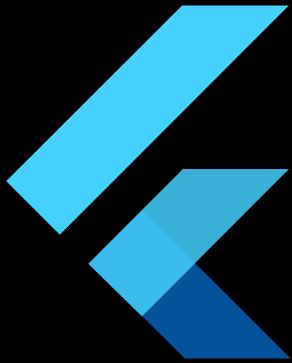


Most popular social networks worldwide as of April 2020,¹⁰
(in millions)



5. Technical Implementation

We Build an App and a DPKI



pub.dev

Getting Started: Flutter ▾ Web & Server ▾

Search Dart packages

web3dart 1.2.3

Published Jan 21, 2020 · simonbinder.eu · Updated: 1.2.3 / 2.0.0-dev.6 · 12 likes

DART NATIVE FLUTTER ANDROID IOS

Readme Changelog Installing Versions 91

web3dart

A dart library that connects to interact with the Ethereum blockchain. It connects to an Ethereum node to send transactions, interact with smart contracts and much more!

Features

- Connect to an Ethereum node with the rpc-api, call common methods
- Send signed Ethereum transactions
- Generate private keys, setup new Ethereum addresses
- Call functions on smart contracts and listen for contract events

Publisher simonbinder.eu

About Dart library to connect to Ethereum clients. Send transactions and interact with smart contracts! Repository (Github) View/report issues API reference

License MIT (LICENSE)



Plasma bags supply chain



A-
A+
B+



B-
AB+
dies



NYU Hospital



Mount Sinai Hospital

Hospital List

OPTIONS

GET ▾

GET /hospitals/

HTTP 200 OK

Allow: GET, POST, HEAD, OPTIONS

Content-Type: application/json

Vary: Accept

[

{

 "id": 6,
 "address": "550 1st Avenue, New York, NY 10016, United
 "hospital_name": "NYU Hospital",
 "city": "New York",

Donor List

OPTIONS

GET

GET /donors/

HTTP 200 OK

Allow: GET, POST, HEAD, OPTIONS

Content-Type: application/json

Vary: Accept

[

{

 "id": 1,
 "ethereum_address": "0x15c5C2ec7Ee2e07F568d922C7B86355
 "city": "New York",
 "birth_date": "1999-09-05",

Django REST framework

```
GET /doctors/
```

HTTP 200 OK

Allow: GET, POST, HEAD, OPTIONS

Content-Type: application/json

Vary: Accept

```
[  
  {  
    "id": 3,  
    "complete_name": "Doctor 1",  
    "license": "3GV7RSE07HJ8mQB",  
    "ethereum_address": "0x6F9567Ef74D62651B6cFfCE0a14Dd21",  
    "three_box_profile": "https://www.3box.io/0x6f9567ef74",  
    "hospital": 6  
  },  
]
```

Django REST framework

```
GET /hematologists/
```

HTTP 200 OK

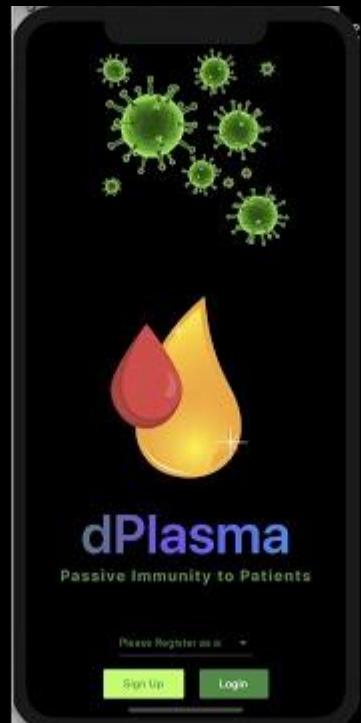
Allow: GET, POST, HEAD, OPTIONS

Content-Type: application/json

Vary: Accept

```
[  
  {  
    "id": 2,  
    "complete_name": "Hematologist 1",  
    "license": "tRHhf8YusNrL75X",  
    "ethereum_address": "0xD0D814AA69c7Ed01E912F5a3bA87238",  
    "three_box_profile": "https://www.3box.io/0xd0d814aa69c7ed01e912f5a3ba87238",  
    "hospital": 6  
  }]
```

Link to App Demo can be seen on YouTube



Decentralized Public Key Infrastructure



A-

Neg Serological >> has Covid19 Antibodies
Positive PCR >> not currently infected with Covid
Not twice pregnant
Between 18-60 years old
Not risk group (tattoos/homosexual relations)



A+

Neg Serological >> has Covid19 Antibodies
Positive PCR >> not currently infected with Covid
Not twice pregnant
Between 18-60 years old
Not risk group (tattoos/homosexual relations)



B+

Neg Serological >> has Covid19 Antibodies
Positive PCR >> not currently infected with Covid
Not twice pregnant
Between 18-60 years old
Not risk group (tattoos/homosexual relations)

```
0x1f46a5
16    }
17
18    // ERC721Mintable tokenContract;
19
20    struct Donor {
21        address donorAddress;
22        string city;
23        BloodTypes bloodType;
24        uint256 birthDate;
25        //person must be between 18 and 50
26        uint256 bodyWeight;
27        //person must be heavier than 110 lbs (50kg) to donate
28        uint256 lastDonation;
29        //if date is less than 4 weeks, person is not available to donate
30        bool serologicalTestIsPositive;
31        //if true (and we want TRUE)>>> person has antibodies, if false, not eligible to do clinical trials or donate plasma fo
32        uint256 dateOfFirstSymptom;
33        uint256 dateOfLastSymptom;
34        bool pcrResultIsNegative;
35        //if true (and we want TRUE)>>> person is not infected with SARS-Covid-19, if false, person tested positive hence, pers
36        // bool isActive;
37        // //person didn't donate in the past 30 days and can donate again
38        bool isFemale;
39        bool hadAnyPregnanciesorMiscarriagesMoreThanTwiceIsTrue;
40        //if true >>> risks of TRALI (transfusion-related acute lung injury), person can't donate plasma or she might kill the
41        uint256 lastTattoo;
42        //if date is less than 12 months from now, person can't donate
43    }
44
45    mapping(address => Donor) public donors;
```

Decentralized Public Key Infrastructure



A-

Neg Serological >> has Covid19 Antibodies
Positive PCR >> not currently infected with Covid
Not twice pregnant
Between 18-60 years old
Not risk group (tattoos/homosexual relations)



A+

Neg Serological >> has Covid19 Antibodies
Positive PCR >> not currently infected with Covid
Not twice pregnant
Between 18-60 years old
Not risk group (tattoos/homosexual relations)



B+

Neg Serological >> has Covid19 Antibodies
Positive PCR >> not currently infected with Covid
Not twice pregnant
Between 18-60 years old
Not risk group (tattoos/homosexual relations)

**0x15c5C2ec7Ee2e07F568d
922C7B86355344CBb891**

<https://www.3box.io/0x15c5C2ec7Ee2e07F568d922C7B86355344CBb891>

**0x762a691D41c570bef967
bc845CDFB56aDDeeA5CA**

<https://www.3box.io/0x762a691d41c570bef967bc845cdfb56addeea5ca>

**0x62EcFAcF18b347C6E31
EDB9d1E2c10eF8122d0Bd**

<https://www.3box.io/0x62ecfacf18b347c6e31edb9d1e2c10ef8122d0bd>

Decentralized Public Key Infrastructure

B-

Patient on the ventilator

Covid Infected

Born: 20/Oct/1964

NYU Hospital

Family signed the IND form



AB+

Patient on the ventilator

Covid Infected

Born: 22/Nov/1965

NYU Hospital

Family signed the IND form



A-

Patient on the ventilator

Covid Infected

Born: 10/Aug/1942

Mount Sinai Hospital

Family signed the IND form



```
45     struct Patient {  
46         address patientAddress;  
47         string city;  
48         string hospital;  
49         BloodTypes bloodType;  
50         bool isINDregistered;  
51         //Investigational New Drug (IND) >> sick/terminal patients or family members must sign  
52         //https://www.nybc.org/donate-blood/covid-19-and-blood-donation-copy/convalescent-plasma-information-family-patient-adv  
53     }  
54     mapping(address => Patient) public patients;  
55 }
```

Decentralized Public Key Infrastructure

**0xEb31Af3f23C147090deD4
D263aF369c3B979F4cD**

<https://www.3box.io/0xeb31af3f23c147090ded4d263af369c3b979f4cd>

**0xA534d9853F4f252672c7
D04e12E7474179aC23c**

<https://www.3box.io/0xca534d9853f4f252672c7d04e12e7474179ac23c>

**0xF2D142013F6278b2D14E
616427A094f1f1e69622**

<https://www.3box.io/0xf2d142013f6278b2d14e616427a094f1f1e69622>

B-

Patient on the ventilator
Covid Infected
Born: 20/Oct/1964
NYU Hospital
Family signed the IND form



AB+

Patient on the ventilator
Covid Infected
Born: 22/Nov/1965
NYU Hospital
Family signed the IND form



A-

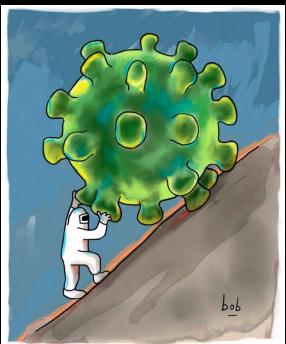
Patient on the ventilator
Covid Infected
Born: 10/Aug/1942
Mount Sinai Hospital
Family signed the IND form



Verifiable Credentials Scheme

**0x6F9567Ef74D62651B6c
FfCEOa14Dd211087B8491**

<https://www.3box.io/0x6f9567ef74d62651b6cffce0a14dd211087b8491>



NYU Doctor



**0x79238629C10E82cAE9
B47E07a144af1684eC81fd**

<https://www.3box.io/0x79238629c10e82cae9b47e07a144af1684ec81fd>



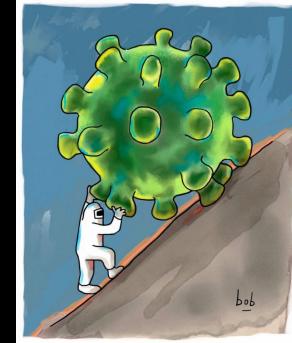
Mt Sinai Doctor



Verifiable Credentials Scheme

**0xBcF4f278d9c801f3386B
C5328553417f4d600043**

<https://www.3box.io/0xbcf4f278d9c801f3386bc5328553417f4d600043>



**NYU Doctor
NYU Hospital**

**0x5ACE75F86123b7434f9
Da8A1459886d74Bdc5fb2**

<https://www.3box.io/0x5ace75f86123b7434f9da8a1459886d74bdc5fb2>



**Mt Sinai Doctor
Mt Sinai Hospital**

Verifiable Credentials Scheme

**0xBcF4f278d9c801f3386B
C5328553417f4d600043**

https://www.3box.io/0xbcf4f278d9c801f3386bc53_28553417f4d600043



NYU Hematologist - works for NYU Hospital in the morning

**0x5ACE75F86123b7434f9
Da8A1459886d74Bdc5fb2**

<https://www.3box.io/0x5ace75f86123b7434f9da8a1459886d74bdc5fb2>



Mt Sinai Hematologist - works for Mt Sinai Hospital in the evening



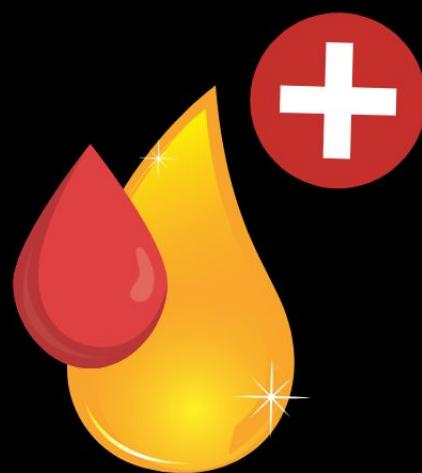
Hematologist is authorized to request/receive Blood Components to the Blood Bank

Hematologist PubKey

0xD0D814AA69c7Ed01E912

F5a3bA87238250B40Db5

<https://www.3box.io/0xd0d814aa69c7ed01e912f5a3ba87238250b40db5>



NYU Hematologist - works for
NYU Hospital in the morning



Mt Sinai Hematologist - works for
Mt Sinai Hospital in the evening

Hematologist has Verifiable Credentials

Signs transactions with his/her PubKey

Hematologist PubKey
0xD0D814AA69c7Ed01E912
F5a3bA87238250B40Db5

<https://www.3box.io/0xd0d814aa69c7ed01e912f5a3bA87238250b40db5>



3 BOX API Products Partners

hematologistNYU+MtSinai / 0xd0d...40db5

0 Following

About

- <https://nyulangone.org/>
- Thu May 07

Work

- NYU Hospital & Mt Sinai Hos...
- Hematologist

Education

- Harvard University
- Biomedical Sciences
- Hematology
- 1980

```
const BLOOD_TYPES={
```

```
  "AB+": ["O-", "O+", "A-", "A+", "B-", "B+",
```

```
  "AB-", "AB+"],
```

```
  "AB-": ["O-", "A-", "B-", "AB-"],
```

```
  "A+": ["A-", "A+", "O-", "O+"],
```

```
  "A-": ["A-", "O-"],
```

```
  "B+": ["B-", "B+", "O-", "O+"],
```

```
  "B-": ["B-", "O-"],
```

```
  "O+": ["O-", "O+"],
```

```
  "O-": ["O-"] }
```



How the life saving
magic happens?

The supply chain of blood components in
any city of the world

Plasma Compatibility != Blood

Donation



A-

Neg Serological >> has Covid19 Antibodies
Positive PCR >> not currently infected with Covid
Not twice pregnant
Between 18-60 years old
Not risk group (tattoos/homosexual relations)



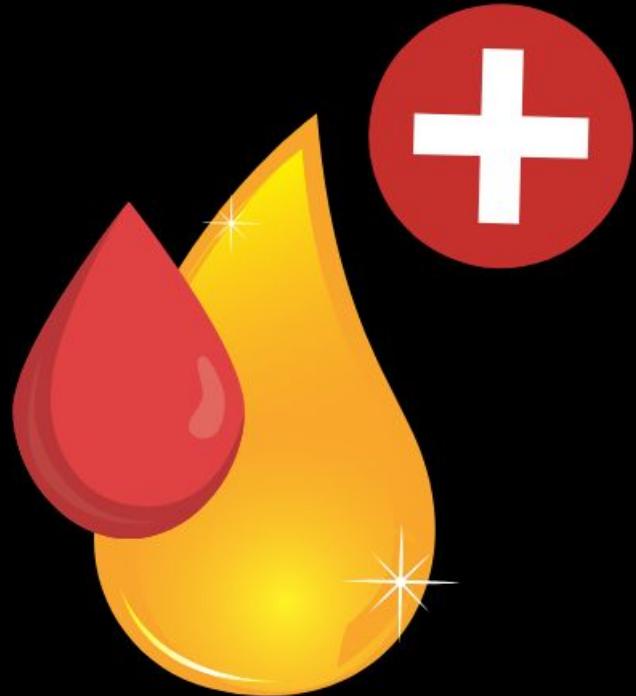
A+

Neg Serological >> has Covid19 Antibodies
Positive PCR >> not currently infected with Covid
Not twice pregnant
Between 18-60 years old
Not risk group (tattoos/homosexual relations)

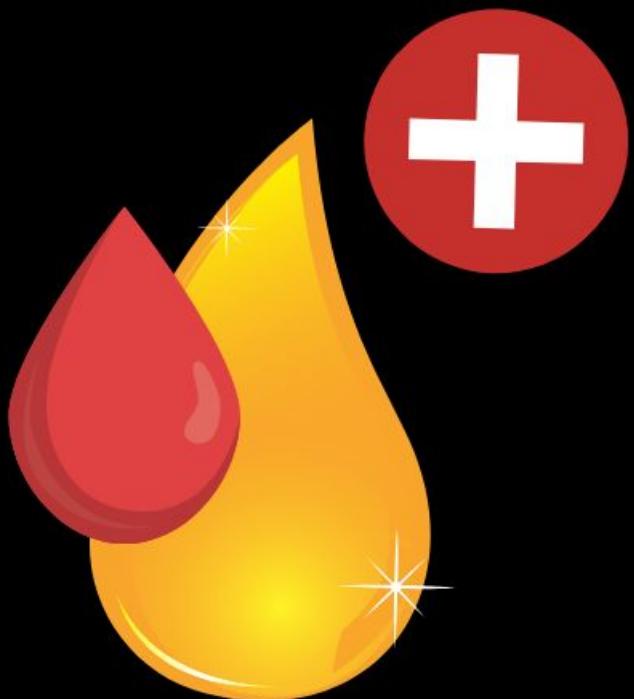


B+

Neg Serological >> has Covid19 Antibodies
Positive PCR >> not currently infected with Covid
Not twice pregnant
Between 18-60 years old
Not risk group (tattoos/homosexual relations)



Blood bank inventory today



A-
A+
B+

B-
AB+

A-

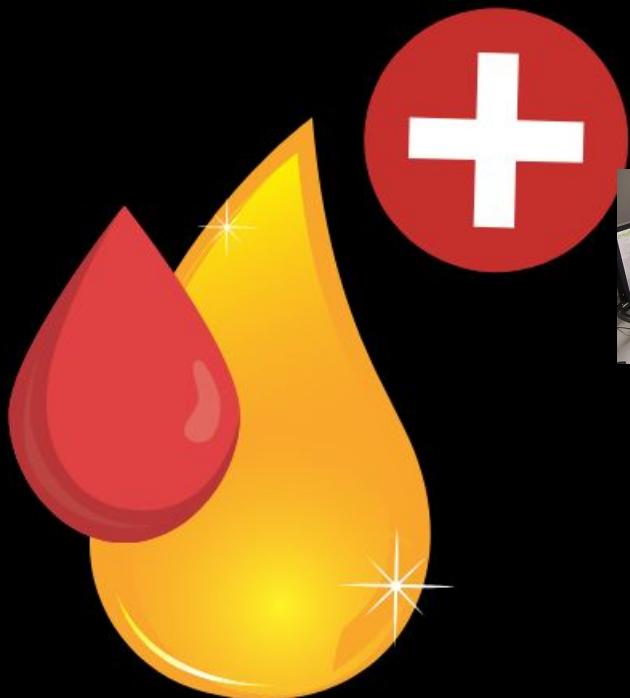


NYU Hospital



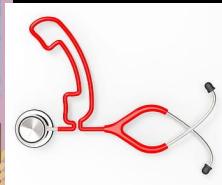
Mount Sinai Hospital

Plasma bags supply chain



A-
A+
B+

B-
AB+
dies



NYU Hospital

A-



Mount Sinai Hospital

6. Value Proposition

AB+ dies, not because of lack of donors

But because the donations on that day, did not match what someone was in need.

An **A+** plasma bag was donated in excess!

Estimation that 20% of plasma/platelets bag are wasted in Canada every year.

Shelf life is 3 days in room temperature - risk of airborne infections

DONORS AND PATIENTS MUST BE ABLE TO MATCH - dPLASMA

Guided donations>>> Donor is required to go to blood center because he receives a phone call.
Manual process, can be automatized. - **dPLASMA**

App acts as a facilitator, using verifiable credentials



Thanks to PubKey/PrivateKey infrastructure, we can authorize only the hematologist to make that “**plasma bag request**” to the Blood Bank

And the BloodBank can verify that that signature is actually corresponding to the Public Key of the hematologist.

App represents the Smart Contract dPlasma.sol deployed at Rinkeby using Ox..... Address

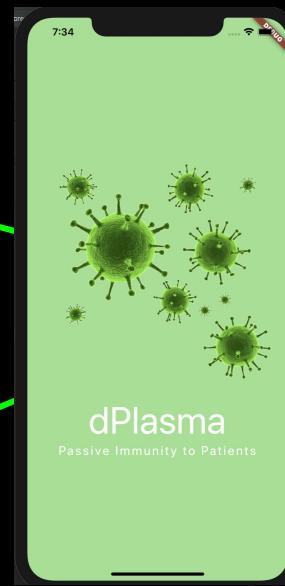
App consumes the Abi.json

```
221 // donations scheduled
222 // called by donors
223 function donationScheduled(address patientAddress) public {
    require(
        donors[msg.sender].donorAddress != address(0),
        "Caller is not a donor"
    );
    require(
        patients[patientAddress].patientAddress != address(0),
        "Patient does not exist"
    );
    //require(bloodBanks[msg.sender].bloodbankAddress != address(0), "Blood Bank does not exist"
    //criou o struct na memoria
    Donation memory newDonation = Donation{
        msg.sender,
        false,
        patientAddress,
        msg.sender,
        address(0)
    };
    donationCount++;
    // gravou o struct no mapping (estado)
    donations[donationCount] = newDonation;
    // 2db event
    emit Donated(msg.sender, patientAddress);
}

modifier onlyBloodBank {
    require(
        bloodBanks[msg.sender].bloodbankAddress != address(0),
        "Caller is not a blood bank"
    );
}

// donations executed
// called by banks only
function donationHappened(uint256 donationId) public onlyBloodBank {
    Donation storage donation = donations[donationId];
```

Now & soon (with your help)



Plasma
donation

Vaccine
development

Full blood
donation

Future uses, e.g. organ
donation, tracking,
bone marrow

Connection to healthcare sector
Business development support
\$120,000 for app & business development

Who pays & why?

- Transfusion services, Hospitals
- OneBlood, RedCross
- CPP Companies/Startups
- Laboratories, Health Insurance Companies

The App will provide:

- Reduction in donor acquisition costs
- Solving a Supply Chain coordination
- Reduction in healthcare costs
- Reduction of long-term healthcare needs



More lives saved
&
\$457,000 savings per surviving patient
(early treatment start at mild stage)

Size of the Market in the US

Potential long-term (post-pandemic) US customers

- **71** AABB-accredited transfusion services
- **862** FDA-registered plasmapheresis centres

Example of pandemic-specific US relationship

2,178 sites in 'COVID-19 Expanded Access Program' to collect and provide convalescent plasma (Mayo Clinic-led) *

→ **12,176** patients >> **7,205** infused

Plasma specialist supplier **Grifols**

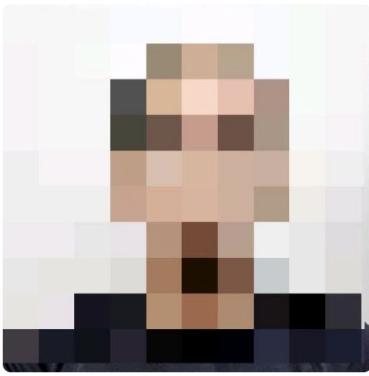
295 donation centers globally. Over **45,000** donations daily.

Plasma specialist supplier **Kedrion**

Kamada-Kedrion global collaboration for IgG product involves antibody specialists in market.

* Data valid as at 8 May 2020, <https://www.uscovidplasma.org/>

8. Team



Ivan Amaro

iramaro

Follow

Writer, developer and blockchain student.

Status.im:

0x04244e395465f0d762440029de7d0a
373f04e1e033c8f63c3c8e10ada9df3274
e798cb100e965678a684b21c9a6a13e97
a9acad94

@blkb-tech

Paraguay

<https://gitlab.com/iraamaro>

Block or report user

Organizations



133 contributions in the last year





 completing-unfinished-Projects

DHRUV MALIK

GrandGarcon

[Follow](#)

Cybersecurity and Fintech enthusiast| loves implementing innovative systems on cybersecurity and DLT for web3.0.

 @EcolePolytechnique

 Paris

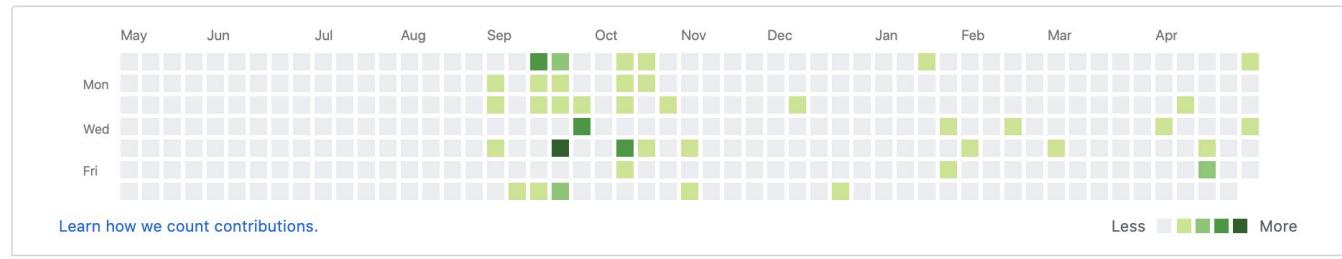
 [DhruvMalik.github.io](https://github.com/DhruvMalik)

 PRO

[Block or report user](#)



77 contributions in the last year





🎯 Focusing

It's Encrypted

itsencrypted

Edit profile

Web3 Dev wannabe

👤 @itsencrypted

📍 Sao Paulo

🔗 <https://itsencrypted.com>



270 contributions in the last year

Contribution settings ▾





You're not the only one cursed with knowledge

Bruno Eleodoro Roza BrunoEleodoro

[Unfollow](#)

Stop thinking, start building !
0xDd6d37E29294A985E49fF301Acc808
77fC24997F

IBM
 SP -Brazil
 brunoeleodoro96@gmail.com
 <https://brunoeleodoro.com>

PRO

Block or report user



652 contributions in the last year



Thank you!



Juliana Passos

Flutter & Smart Contract Developer



Bruno Eleodoro

Flutter Developer & DevOps



Ivan Amaro

Backend Developer - Data Science



Dhruv Malik

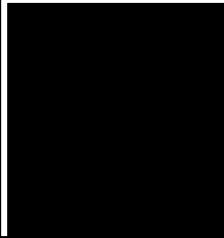
Backend Developer - Data Science



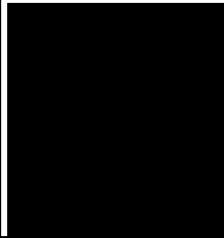
Dr Chris Wirrig

Mentor - Biomedicine



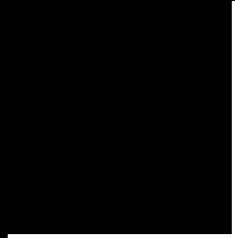


Thank you!



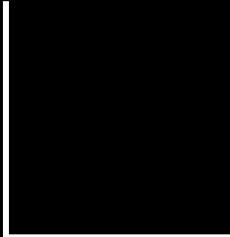
More information

Bibliography



dPlasma's Idea

1. Building something useful
 2. Simulations based on real life problems
 3. Allowing Scientists to access Blockchain data
 4. Protect Donor's sensitive information
 5. Match compatible donors & recipients
-



Antibodies - generating a proof

An Antibody Test, a.k.a Serology Test analyses a patient's serum - the liquid portion of the blood that excludes cells and clotting factors but includes antibodies.

Polymerase Chain Reaction (PCR)

The way we're testing infections right now is by looking for viral genetic material in patients samples. Using a method called Polymerase Chain Reaction (PCR), clinicians can amplify any coronavirus RNA in a patient's nasal swab so its presence can be confirmed.

Viral DNA & RNA can be found in the body as soon as an infection begins, even if you're asymptomatic.

Serological Tests

Antibodies, aren't developed until several days after the infection has taken hold. They are around the blood in large numbers for many months after the infection.

Not a useful indicator of who is currently infected.

EXTREMELY USEFUL: To identify past cases long after the infection has been beaten.

Costs: less than \$10 (Company: Biomerica)

Results ready: in just a few minutes

Accuracy: 87.3% sensitivity (below benchmark)

PCR Tests

Viral DNA and RNA can be found even if you're asymptomatic

Disappears soon after the immune system clears the infection out.

USEFUL TO: Find out who is **CURRENTLY INFECTED**, but not who once was infected.

Costs: up to \$51 under Medicare

Takes hours to run the test (shipped back & forth from testing site) >> Patients gets the results within a few days.

Accuracy : high

Antibodies Tests - Limitations

An antibody test will show
that someone is immune, but
it doesn't guarantee that the
person is no longer
contagious.

Ideal Scenario

You need both PCR & Serological Tests

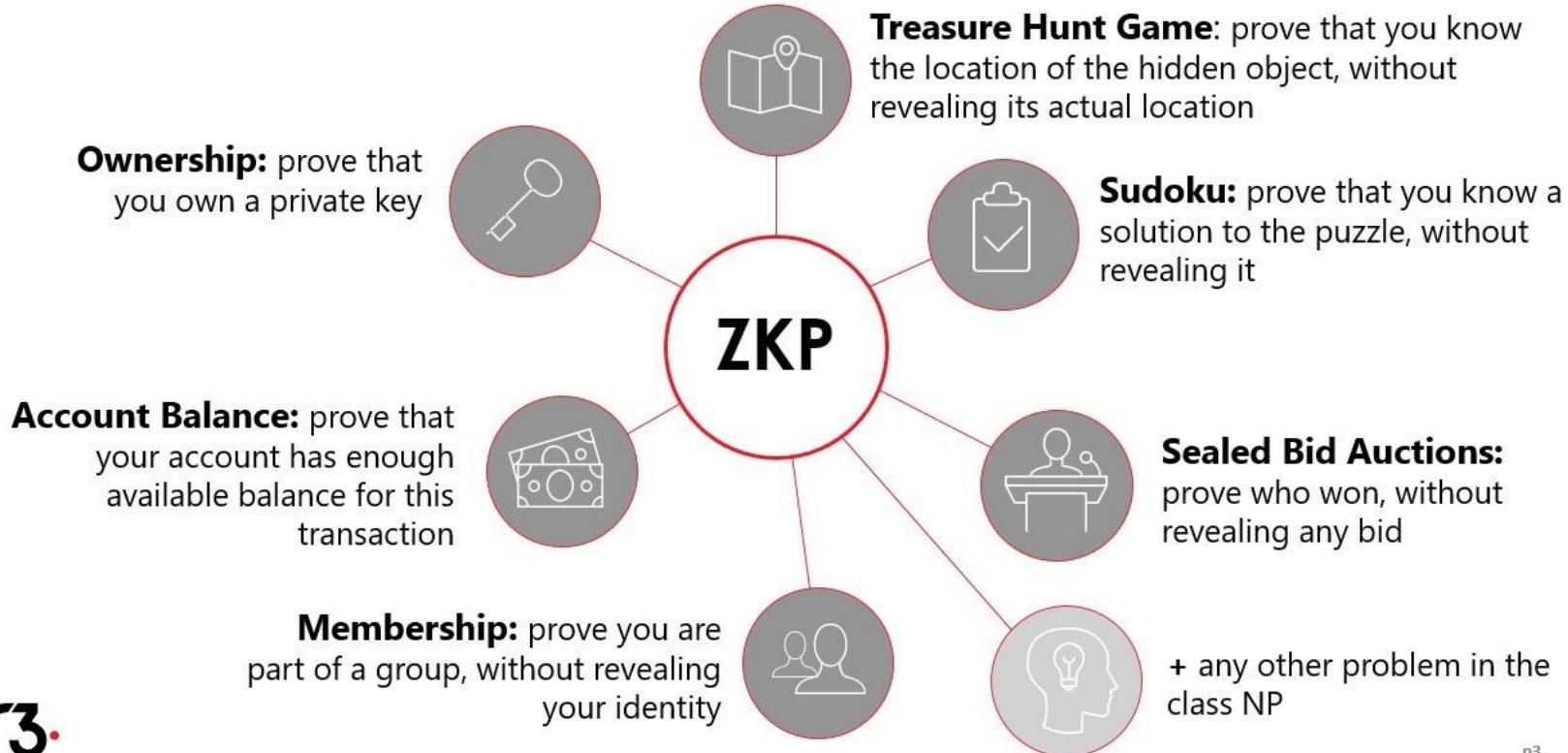
Test positive for immunity = “Proof of Antibodies” in the Serological Test

AND

Test negative for the virus in the PCR test (= my current state of health today)

Zero Knowledge Proofs

Applications of ZKP



PROVER

Demonstrates that they performed a calculation on a set of inputs, without revealing some of those inputs.



Zero-Knowledge proof is a mathematical expression that is carried out by the prover and verifier. There can be many provers and verifiers for one ZKF protocol.

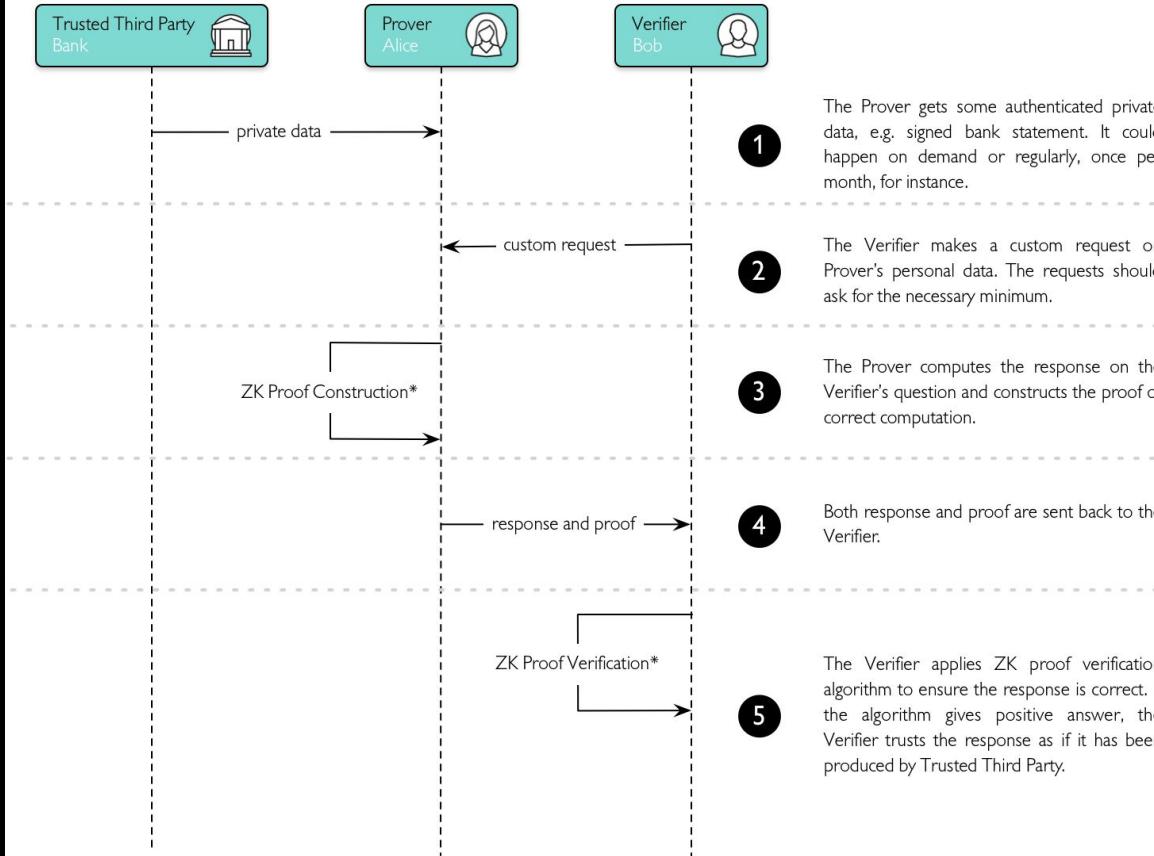
“Hello Oxb40ebf27fBDc179d04B8ad76C407F19BaF39A8F8, can you prove that you tested positive IgM and/or IgG for COVID-19 and that you meet all the donor eligibility requirements (21 CFR 630.10, 21 CFR 630.15) ?”

VERIFIER

Can verify that the specific statement sent by the prover is true. Verifier constantly asks series of questions about the “knowledge” the prover possess.



Zero-knowledge Protocol: Data Exchange

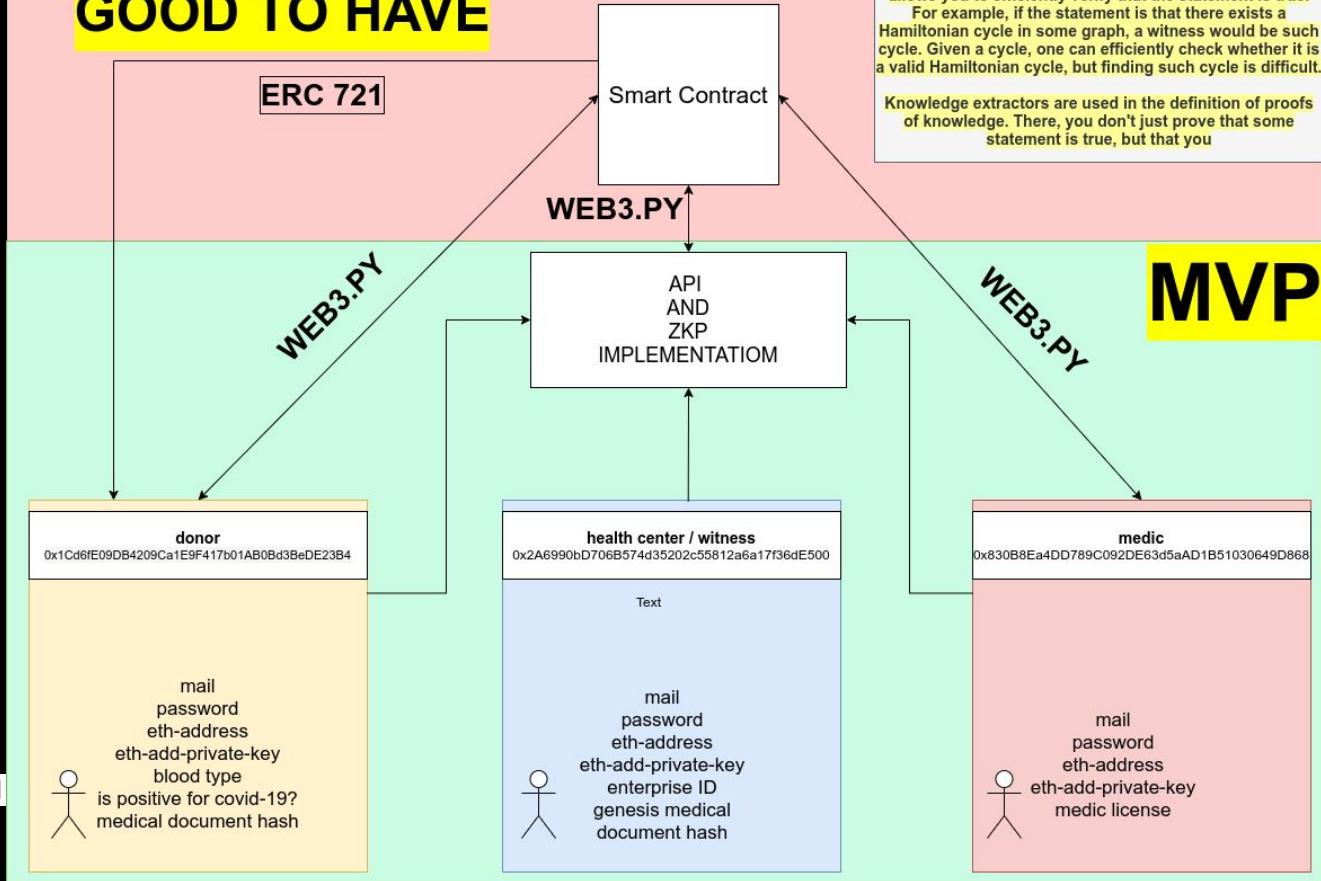


* ZK proof construction and verification algorithms are detailed separately

GOOD TO HAVE

A witness for an NP statement is a piece of information that allows you to efficiently verify that the statement is true. For example, if the statement is that there exists a Hamiltonian cycle in some graph, a witness would be such cycle. Given a cycle, one can efficiently check whether it is a valid Hamiltonian cycle, but finding such cycle is difficult.

Knowledge extractors are used in the definition of proofs of knowledge. There, you don't just prove that some statement is true, but that you



0x2A6990bD706B574d35202c55812a6a1

<https://faucet.rinkeby.io/>

Bruno Eleodoro Roza 10:08 PM

0x830B8Ea4DD789C092DE63d5aAD1B51030649D868

Ivan Amaro

0x1Cd6fE09DB4209Ca1E9F417b01AB0Bd3BeDE23B4

Testing Testing Testing Testing...

Individuals without severe symptoms are being turned away for testing. => NO WAY TO KNOW if they were once sick and now potentially immune, or still at risk of being sick and spreading the virus.

If you're not able to test everyone, we have no way to
to know:

- how widespread the infection is;
- what the true fatality rate is;
- what kind of measures to stop the spread are
actually working.

How do Antibodies act?

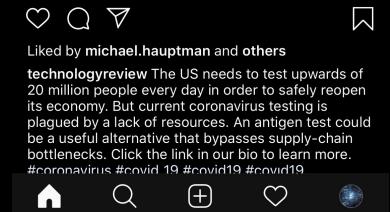
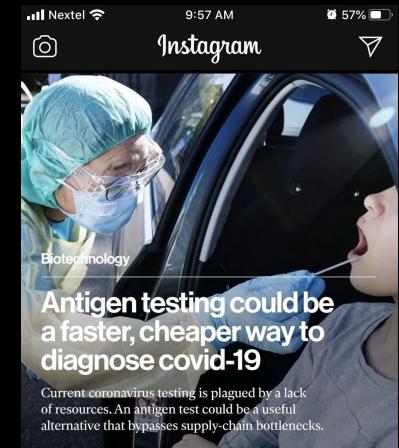
When the body is introduced to a pathogen, the immune system develops tailor-made antibodies that act against the infection.

Antibodies can last a long time, from a couple of years to a lifetime, depending on the disease.

Serology Tests

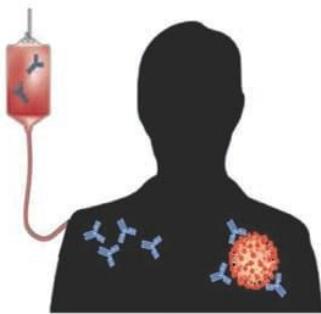
ACCURACY of Serological Tests

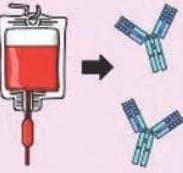
ELISA (Enzyme-linked immunosorbent assay) : Clinicians look for antibodies that were made in response to the large protein that sticks out of the coronavirus surface.



Passive Immunity

Passive immunization



PASSIVE IMMUNITY	
Natural	Artificial
 Maternal antibodies	
	 Monoclonal antibodies

Passive Immunity

Develops after you receive antibodies from someone or somewhere else

Natural

Antibodies received from mother, e.g., through breast milk



Artificial

Antibodies received from a medicine, e.g., from a gamma globulin injection or infusion



S

1. creating end 2 end automated workflow of plasma test reports w/ verifiable credentials and supply tracking ensures ease for donors to donate hassle-free
2. Simplified UI for reducing time for patient registration .

W

1. FHIR is a centralised database and thus bleak chance of sudden outages
2. needs to decrease the gas cost per transaction (as currently we need to decrease the patient params to avoid the gas limit).
- 3.

O

1. can be scaled to multiple tests as the data transaction layer is modular to include more parameters of tests for particular patient
2. DPKI with governance for hospitals and bank
3. using ZkSTARKS / zokrates for implementing DPKI.

T

1. Patients data surveillance
2. Stability of main-net .

architecture of backend API implementation (Credits Ivan)

1. accessing endpoints

Using the URLconf defined in `api_dplasma.urls`, Django tried these URL patterns, in this order:

1. `admin/`
2. `^hospitals/$ [name='hospital-list']`
3. `^doctors/$ [name='doctor-list']`
4. `^patients/$ [name='patient-list']`
5. `^hematologists/$ [name='hematologist-list']`
6. `^donors/$ [name='donor-list']`

Some examples of queries from the anonymized FHIR Database interacting with frontend database for verification .

1. For Donors

```
GET /donors/
```

```
HTTP 200 OK
```

```
Allow: GET, POST, HEAD, OPTIONS
```

```
Content-Type: application/json
```

```
Vary: Accept
```

```
[
```

```
{
```

```
  "id": 1,
```

```
  "ethereum_address": "0x15c5C2ec7Ee2e07F568d922C7B86355",
```

```
  "city": "New York",
```

```
  "birth date": "1999-09-05",
```

2. For Doctors / hematologists etc.

```
HTTP 200 OK
```

```
Allow: GET, POST, HEAD, OPTIONS
```

```
Content-Type: application/json
```

```
Vary: Accept
```

```
[
```

```
{
```

```
  "id": 3,
```

```
  "complete_name": "Doctor 1",
```

```
  "license": "3GV7RSE07HJ8mQB",
```

```
  "ethereum_address": "0x6F9567Ef74D62651B6cFfCE0a14Dd21",
```

```
  "three_box_profile": "https://www.3box.io/0x6f9567ef74",
```

```
  "hospital": 6
```

PROBLEM 1: Verifiable credentials are necessary in the current system (DATA VALIDATION/INTEGRITY) - Super verification is needed

PROBLEM 2: Getting the correct donor for the correspondent patient (COMPATIBILITY/MATCHING)

PROBLEM 3: too much bureaucracy (ex. India), long chain of process. Verification is not efficient. (INEFFICIENCY of THE SYSTEM + BUREAUCRACY)

PROBLEM 4: Saving the privacy of potential donors is important in certain countries. (GDPR - disclosing genetic info is restricted) >> HOSPITALS NEED AN IT OFFICIAL (Written consent of the patient is needed) >> (DATA PRIVACY/INTEGRITY (not corrupted data))-

Verify the potential donor to donate their plasma.

Simplify the process scalable solution, using ZKP.

Clinics get the data, get potential donors without any hassle. Clinics do get the data - backlog of treated patients (weeks to 10 days to get the form verified, that they got ZKP allows multiple parties to prove a certain fact (potential donor) >> asserts the facts that he fills all the requirements of potential donors. >> Sick patients of potential hospitals.

Saving the privacy of potential donors is important in certain countries. Donors, proof of donation, in the blockchain. Healthcare medics, potential recipients in the plasma bag.

Different officials can later check the data via Blockchain from the GDPR standardization. One will be able to use ZKP and validate the

**Problema: Encontrar os potenciais doadores de plasma para os pacientes, pessoa do tipo O-
(COMPATIBILITY/MATCHING)**

We are using Ethereum, bc all the mapping of data that is being used by the scientist community to identify the potential donors >> Put the potential donors in Ethereum.

Problem: vaccine is taking a long time (VACCINE will take time)

Quarantine is the current treatment. Plasma from really recovered from donors. >> Clinical Trials are going on and they need plasma donors

Inject that plasma. A doctor ran out of options (use CPP plasma in terminal patients justifies)with Covid 19 is looking for

PROBLEM We have a lot of data, we're trying to match with people with antibodies, with people that need these antibodies. (MATCHING)

Trying to verify that this person recovered from Covid 19. (VERIFICATION OF EXAMS - Data can be corrupted in the document) / FHIR uses oAUTH (username/pwd - GoogleAuth - encrypted data) - verification of exams (potential donor enters the details in the form - medical institution / testing lab is connected to FHIR Database) >> data fetched is the same as local data (FHIR is centralized)

Using ZKP, we can prove and verify that this person has the antibodies, based on a verifier.

PERSONA: Is afraid that your disclosing your genetic for a “useless” study

Is already a long time blood donor

Donor is altruistic (expects no reward back) - donates to recover blood bank to recover inventories.

Believes that sending for the benefit science/progress is OK, but...

No disrupt of finality...and my genetic data would be used commercially (big data capitalization that he is not ok) -

Adoption of bone marrow (transplant)

Believes in the doctors that will analyse his data are going to do good with his data. (communication between researchers and donors) - Get to choose what your info will be used for

Matching donors with people that need

Clinical trials need a lot of data (big sample is necessary)

FHIR >>> We get data from a public database in the US

CPP >> is only for terminal patients, not a proof of immunity

Proof of antibody (PCR + Serological tests)

We need to figure out a way to connect the compatible people (donors/recipients)

1Up Health API

Framing of the Problem

1. MATCHING DONORS-PATIENTS (finding perfect compatibility)
2. STATEMENT: Clinical trials need a lot of data (big sample is necessary) >>> for accuracy (lots of data are necessary)
3. Generate a Proof of antibody (PCR + Serological tests)
4. 1upHealth >> patient gets rewarded for providing their data (Apple/Google provide them the data) / 1Up health (user disclaimer) >> CENTRALIZED PERMISSIONED (you need permission to access it) DATABASE - NOT ON THE BLOCKCHAIN - FHIR is not global - (FHIR / DATA LEAK) - (Cybersecurity must be strong) Technical Competence and Capabilities/Weight 20% The demonstration addresses the primary goals of the Stop CoVID-19 Hackathon and exhibits interoperability with existing blockchain technologies with an emphasis on the Ethereum blockchain.

Websockets from potential donors to potential recipients - in order to communicate with each other will be complex (make it scalability) >> centralized (FHIR house) (scalability not an issue, security is!) >> hashes in the blockchain with patients ID, centralized WebApp (sending hashes for proof). >> oAUTH (only have access to your data, you log in with your credentials, people use their Google credentials) (Ex. 100 users logging in to give their token) >> API Key (expiration key is forever, no need to "annoy" the user) >> Control on the hands of the user with OATH (you can simply disconnect) >> OAuth >> You need a HUMAN to do the authentication (you have to type the password) - oAUTH uses your authentication App (2FA)

Ethereum / Hyperledger - current hospitals have old PCs, not progressing to using blockchain (worldwide data, permissioning system >> verifiable credentials) >> consistent profile of a particular person / CONSISTENCY - STANDARDS of FHIR are good, can be expanded to the world (QR code, scans GPS location, pandemic area) >> consensus of multiple data sources ->> ETHEREUM >> bigger network, the bigger it is it is more secure, and it is free (leak of data in private db vs. security of Ethereum nodes)

5. What is it for?

We can

Doctor John-
PK -
0x2A6990bD706B
574d35202c55812
a6a17f36dE500

Precis
1 de 0-

Mount Sinai Hospital - PK:
ethereum address - not sufficient to prove
that it is a trusted entity (attestation
that each hospital is authorized)

Doctor John- PK -
0x2A6990bD706B574d
35202c55812a6a17f36
dE500

NYU Hospital - PK >>>
Preciso de alguem tipo
B+

BLOOD BANK - onibusinho:
Blood banks matching patients and
donors - redirect their plasma bags to
the hospitals nearby

Patient PK:
0x134BF142f5
25F3383c4770
f2e95EeF7430
7aBb24

DATA CONSUMERS:
Anyone interested in buying
genetic data of people. (You
buy ATGCATCGATCG), without
knowing Who they are

Fluxo May 2nd

Unicornio Donor1 doa plasma tipo A-
Unicornio Donor2 doa plasma tipo A+
Unicornio Donor3 doa plasma B+

hospitalNYU tem:
1 paciente precisando de plasma B (pode receber do Unic3)
e 1 paciente precisando do tipo AB (nao teve Unicornio >>
morreu!!) - RIP

Mont Sinai Hospital has:
1 patient needing A (pode receber de Unic1, Unic2)

Patient Group	Compatible Plasma Donor
A	A, AB
B	B, AB
AB	AB
O	O, AB, A, B

Plasma compatibility

Plasma contains anti-A and anti-B antibodies depending upon the blood group. Our body also has antibodies to A and/or B antigens according to our blood group. Patients should only receive plasma that does not contain an antibody which could attack the antigens present on their own red cells.

Group A recipients have A antigen on their red cells, so they can't receive group O or group B plasma as the anti-A will attack their red cells. Group B recipients have B antigen on their red cells, so they can't receive group O or group A plasma as the anti-B will attack their red cells.

Group AB recipients can only receive group AB plasma. Group O recipients do not have either A or B antigen, so can safely receive plasma of any blood group type.

Smart contract - ordem cronologica das paradas

No 3Box

Criar: NYU Hospital, Doador1, Da

```
0xA37171CEc55edd14B96660446665eD407Cb2D028 (NYU Hospital) >>> pode assinar tx como hematologista??
```

```
>>> NAO
```

```
donorSignUp{
```

```
Cidade,
```

```
bloodType,
```

```
serologicalIsPositive
```

```
}
```

PROBLEM

Matching donors/patients >> and we need a lot of data for Clinical Trials

Solution: We have a lot of data!! FHIR :-)/ Thanks to uP we were able to take of FHIR filtered precious data... HOWEVER... 1UP is Centralized (has a good OATH), but, cybersecurity is always a risk ... Data leak (??) - Global data >> ETHEREUM >> bigger network, the bigger it is it is more secure, and it is free (leak of data in private db vs. security of Ethereum nodes)

We also have the donor, that cares about the “theft” of his genetic data... BloodType is one step away from genetic data (he doesn’t care to share blood type, but cares to keep his genetic data with him)

The blockchain allows the construction of a DPKI (decentralized public key infrastructure) >>

DocuSign — their own CRM solution (assign different roles to different people).

Ethereum ENS - itsencrypted.eth (Ethereum Name Service).

Exchange of Public Keys via ZKP to do multi-party computation, to generate randomized keys. Trying to generate randomness

- Right to Stop sharing my info (I will get to choose where my info would do good), Decide when to stop sharing - they have the obligation to tell where they are moving my sample/data

GDPR - access behavior via cookies - similar to genetic data (

Likes to receive “recognition”

Why is it important to build it?

0x4f0a1940De411285ad0455a7F40C81B5E0BC8492 >> JU Public KEY >> itsencrypted.eth

0x2A6990bD706B574d35202c55812a6a17f36dE500 >> Alice Public Key

0x2dE863Be86b773011ea601e49e1657E43502562f >>> NYU Hospital

(Rinkeby) C316C0ACACE59FE57909D7974E8E600EBF85433BD7A13FD3F4692EDD5A661497

Hospitais parceiros falam com “buckets de informacao” do paciente (um endereco ETH (pag do site) hospitais mandam tx para esse endereco (com hash de um json nos metadados) - (nessa tx tem: bloodType, gender, testResults)

nao precisa de ZKP (nao precisa desenhar um sistema de login completo) - so demonstra a consulta de web3 do smart contract

Sistema que faz verificacao estatistica (Covid19) - tem interesse em participar? (Vantagens: Rewards em \$\$ - incentive system to install App on mobile phone with his address) - 1) Dados sao aleatorios? 2) forma de dupla validacao dos dados oficiais (DADO para contrastar com o dado MSaude)

Why now?

It's a blockchain solution and the reason why it is being built now is xyz

Can it wait 5 years to be built?

If things can wait to be “faster, better, stronger, more viable, etc” it doesn’t need to be built now.

Ex: Solve now because>>> this is the global climate and the planet can't wait

Or this population have been suffering for a lot of time, and now finally/potentially we have a solution >> this is why we need to do it now.

Tech Stack

1. **1upHealth** (FHIR Database API) >>> not perfect >>> we need ETHEREUM >> (API >> I don't get genetic data, symptoms, bloodType) - information confinement HIPA - legal framework dedicated system - sophisticated hacker will leak their system (database we have is secure) - legal part // not part of the project (APIs - grabbing patient's data) - Bruno (May 5th on)
2. We don't know if Roberto's data is being sold to 3rd parties? >>> ETHEREUM (XXXX)
3. Smart Contract - Development
4. Status - () - data hash table technology (acc creation), password, eth add and pseudonym
5. Check 3Box (repo), / Adding 2FA (Senior managers) - OTP (another layer of KYC) -
6. BY THURSDAY - verifiable credentials

Next Weekend: 9 / DELIVERY DAY: 10

VERIFIABLE CREDENTIALS ...

DPKI (drawings) - images / personas (UI) >> Juliana until Thursday

SLIDESHOW

Front end - React / Flutter

Nodejs / Abi.json / >>> come together (integration back to front)

Blockchain

Is it imperative to use the Blockchain? A permissioned database could do it?

Is it nice to have? Not necessary, but nice to have..