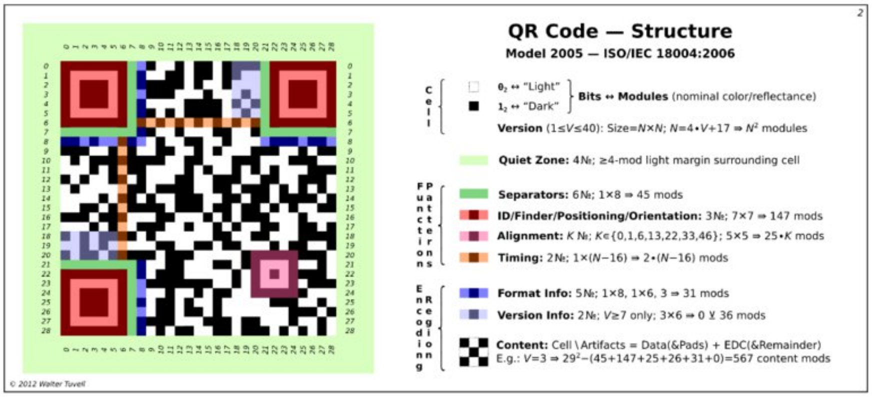
Physiognomy Research

From the Greek '***physis***' (nature) and '***gnomon***' (judge)

Formal Definition: Assessment of character or personality from a person's outer appearance, in particular the face.

QR Codes

The QR Code was developed in 1994 by a company called Denso Wave, in order to track vehicles during manufacturing. It was designed to allow high-speed component scanning. The traditional barcode was one-dimensional, allowing for around 20 characters to be encoded into the image. The QR code is two-dimensional, allowing for much more data to be stored within it (around 7100 characters, including numbers, symbols, text, and control codes). Additionally, QR codes are resilient to damage and allow for data restoration. If it is torn or gets dirty, all you would need to scan it is 70-75% of the image.


2
QR Code — Structure
Model 2005 — ISO/IEC 18004:2006
Cell
0_2 ↔ "Light"
1_2 ↔ "Dark"
Bits ↔ Modules (nominal color/reflectance)
Version (1≤V≤40): Size=N×N; N=4•V+17 ⇒ N^2 modules
Quiet Zone: 4№; ≥4-mod light margin surrounding cell
Function Patterns
Separators: 6№; 1×8 ⇒ 45 mods
ID/Finder/Positioning/Orientation: 3№; 7×7 ⇒ 147 mods
Alignment: K №; K∈{0,1,6,13,22,33,46}; 5×5 ⇒ 25•K mods
Timing: 2№; 1×(N−16) ⇒ 2•(N−16) mods
Encoding Region
Format Info: 5№; 1×8, 1×6, 3 ⇒ 31 mods
Version Info: 2№; V≥7 only; 3×6 ⇒ 0 ⊻ 36 mods
Content: Cell \ Artifacts = Data(&Pads) + EDC(&Remainder)
E.g.: V=3 ⇒ 29^2−(45+147+25+26+31+0)=567 content mods
© 2012 Walter Tuvell

Shortcomings of QR Codes

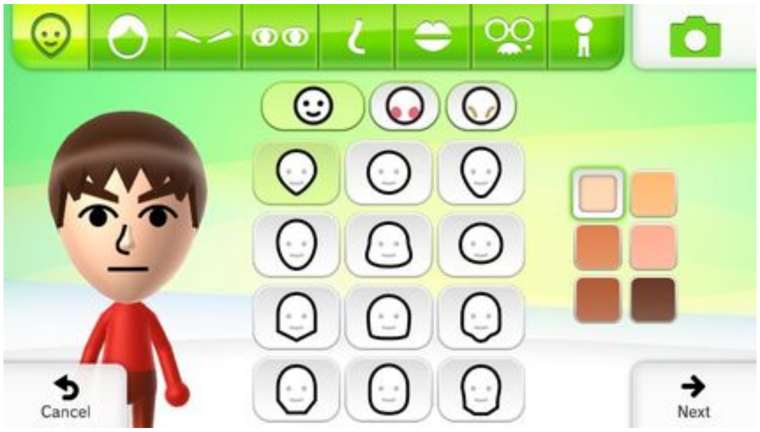
- No way to remember a specific QR code (forgettable)
- Intimidating to non-technical people
- Minimal customization
- No native QR scanner in iPhone scanner
- Delay in processing QR code
- No feedback information sent to QR Code distributor (one-way)
- Unsightly
- Public unawareness

Relevant Examples of Physiognomy

Nintendo Mii

https://en.wikipedia.org/wiki/Mii

With the release of their Wii console, Nintendo implemented a new avatar functionality to act as a digital representation of the player. Allowing for a wide array of customization, these "Miis" are a primitive, basic implementation of a digital identity.

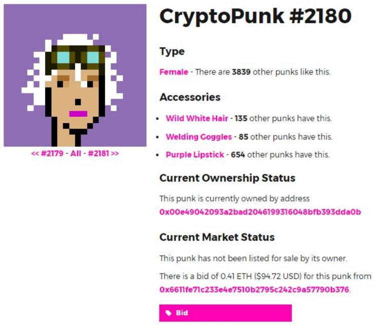


Without displaying a name or ID, a player could be recognized in a party by nothing but their digital avatar.

CryptoPunks

http://www.larvalabs.com/cryptopunks

Larva Labs recently launched an Ethereum project called CryptoPunks. It's an intriguing blend of blockchain use case, artistic expression, and physiognomy. A CryptoPunk is a 24x24 pixel image depicting a face, and there are only 10,000 that exist. No two are exactly alike, and proof of ownership is stored on the Ethereum blockchain. It is described as *almost* an **ERC20 token**, in that it is stored on the blockchain and holds value. Much like the numerous **ICOs** launched lately, you purchase them with ETH and is stored in the address of the owner.



CryptoPunk #2180

Type

Female - There are **3839** other punks like this.

Accessories

- Wild White Hair - **135** other punks have this.
- Welding Goggles - **85** other punks have this.
- Purple Lipstick - **654** other punks have this.

Current Ownership Status

This punk is currently owned by address
0x00e49042093a2bad2046199316048bfb393dda0b

Current Market Status

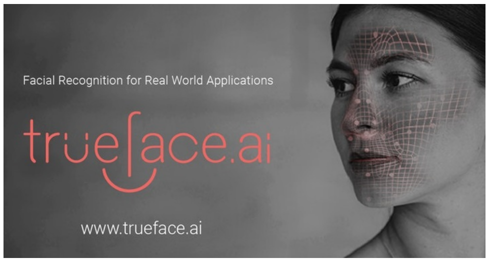
This punk has not been listed for sale by its owner.

There is a bid of 0.41 ETH ($94.72 USD) for this punk from
0x6611fe71c233e4e7510b2795c242c9a57790b376.

Although the faces themselves cannot be scanned to retrieve specific data like QR codes, this concept could be built upon to allow them to have more functionality than just artistic expression. Each face has a set of parameters that can be anything from accessories to emotional expressions. Earrings, bandannas, smiles, glasses, beards, and other features are tracked for every CryptoPunk. This allows for filtering to view only a subset of faces that contain a particular parameter. If this type of customization was tied to a numeric value, then the faces could be a visual representation of data behind-the-scenes.

Existing Facial Recognition APIs

https://www.trueface.ai/



Trueface is a facial computing API that specializes in three services: Facial Detection, Facial Recognition, and Spoof Detection.

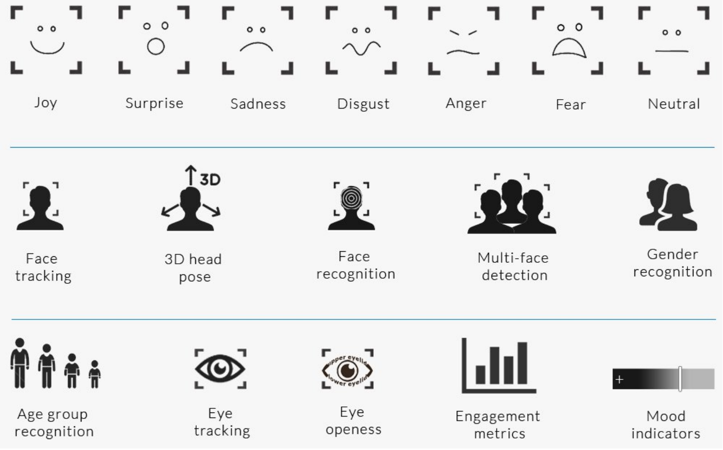
Facial detection does not care about the identity of the person being viewed. For example, a camera can use facial detection to maybe brighten faces in the final version of a photo. It doesn't matter who the picture is of, just that the face is well-lighted and easy to see.

Facial Recognition on the other hand is concerned with the identity of the person, and how their face compares to others. This is extremely relevant as of late with photo organizational software attempting to group photos into albums based on people. An algorithm analyzes the nuances of a persons face, and can then detect that same face in multiple photos or videos.

Spoof detection is a slightly newer concept in the study of digital physiognomy, but will most certainly become more important as the technology advances and becomes more widely used. In order to use facial recognition in secure or sensitive implementations it needs to be accurate. In primitive facial recognition applications, the user could hold a photo of someone else's face in front of theirs to trick the algorithm into false identification. Instead of a photo, the wrongdoer could use makeup, masks, or other techniques to modify their appearance with the intent of circumventing the facial recognition security.

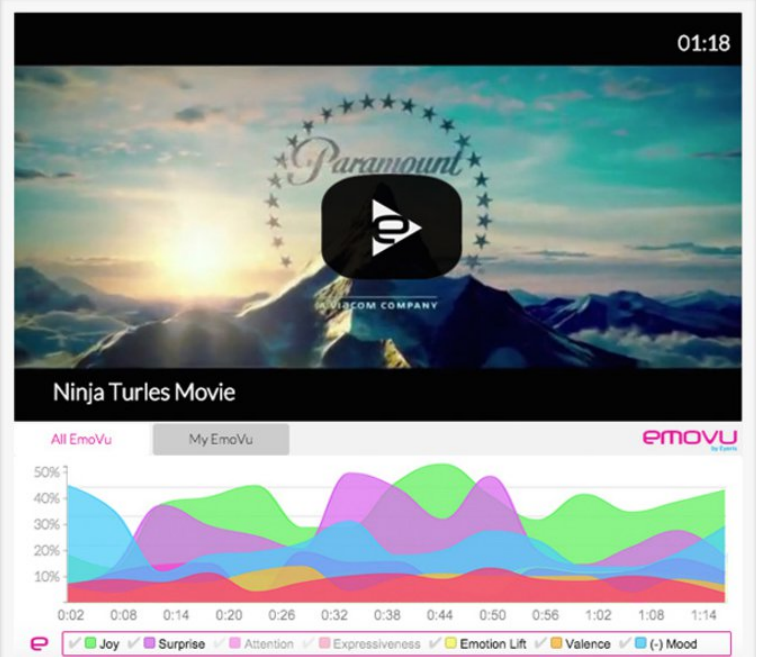
In the future, much more security infrastructure will be using **biometric devices** for authorization. Spoof detection is an integral feature of an enterprise-ready facial recognition API. If the system can be fooled, it risks delegitimizes the entire technology. Right now, facial recognition is still viewed as gimmicky by the mainstream public. It is simply used to organize photos in iPhoto, or add a funny filter in Snapchat. However, recent adoption suggests that in the future our passwords will be ingrained in our biology. For it to be viable in more serious applications, the API and algorithm need to be airtight.

http://emovu.com/e/

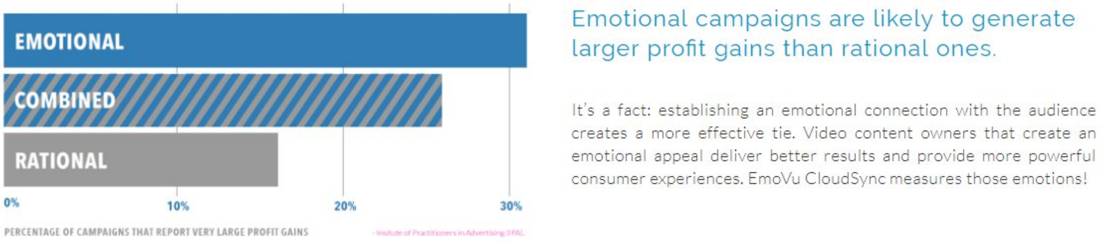


EmoVu by Eyeris takes facial recognition to a whole new level. Facial cues correspond to emotion. It is how we interact with people everyday. When we talk to someone, our eyes analyze their facial response and then our brain tried to deduce the emotion behind the facade. Some emotions are easily categorized. A frown is probably highly correlated to displeasure, while a smile is highly correlated to happiness. However, there are a multitude of facial manipulations that are indicative of an wide array of emotions. EmoVu aims to quantify the **metadata of emotion**. If you thought a company knowing your email was bad, imagine if they knew exactly how you felt when viewing a piece of content.

EmoVu claims that they “bridge the gap between emotion recognition, face recognition, age & gender identification, eye tracking, gaze estimation and everything else in between”. This is a robust type of emotional analytics that has not been seen yet in the field of **Human-Machine Interaction (HMI)**. They can attach the API to a video, and track how each person feels throughout the content. When all of that data is aggregated, you get a graph of the pubic's emotional response to something over time:



This type of personal information would be invaluable to advertisers when trying to reach their audience. For an eternity, content creators have had to guess how an audience would receive their subject matter. This new emotional appraisal removes uncertainty and demystifies the human component of marketing. It allows corporations to precisely calculate exactly how and who they want to target. The EmoVu website even claims:



-Insitute of Practitioners in Advertising (IPA).

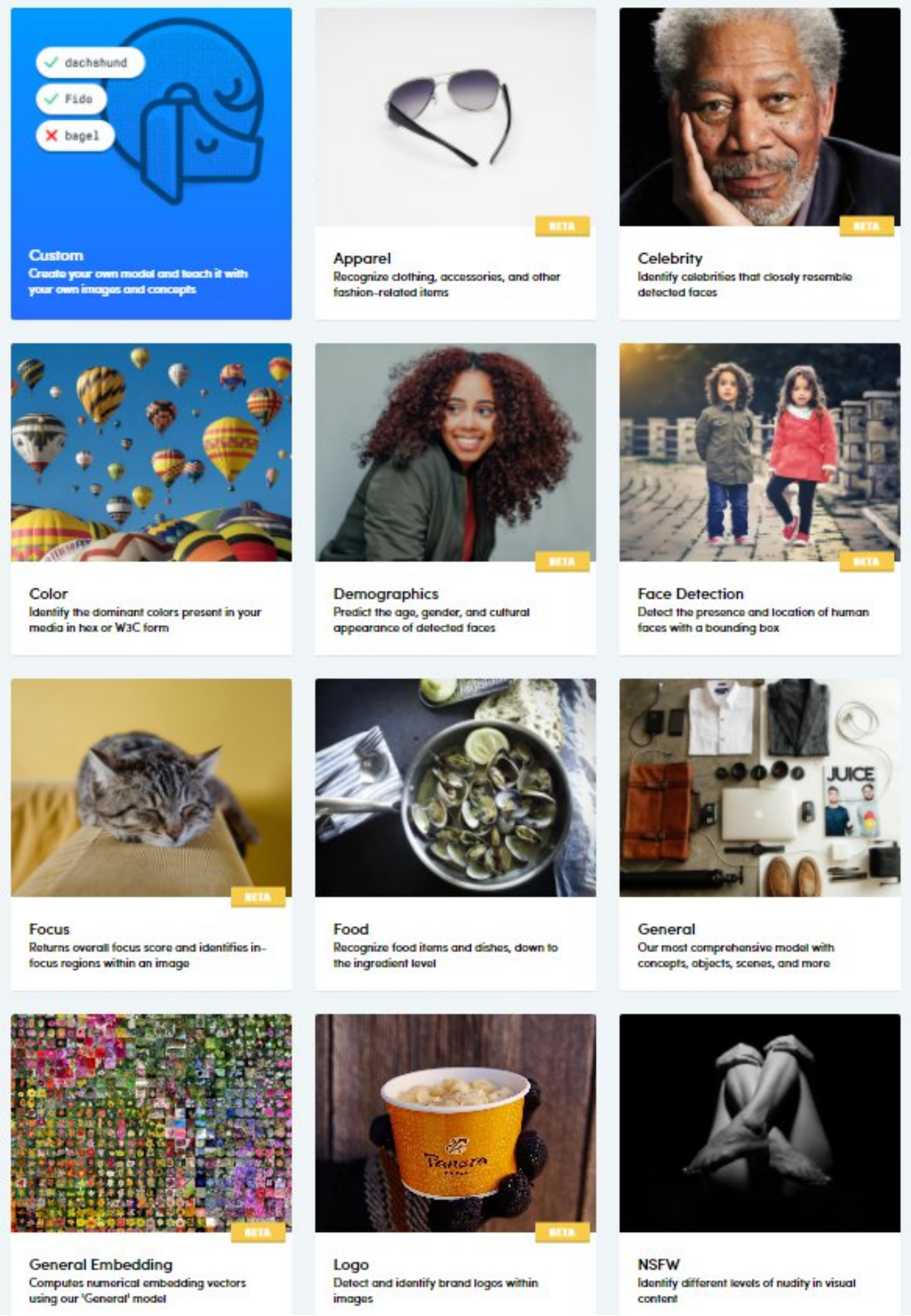
Emotional campaigns are likely to generate larger profit gains than rational ones.

It's a fact: establishing an emotional connection with the audience creates a more effective tie. Video content owners that create an emotional appeal deliver better results and provide more powerful consumer experiences. EmoVu CloudSync measures those emotions!

Advertisements are no longer a unidirectional form of propaganda. Now, information can be sent back to the advertiser informing them of how their campaign is being received. This will enable fine-tuning a piece of content to elicit the most evocative response possible. They call this **Ambient Intelligence**, which is a devices passive ability to establish contextual awareness.

https://clarifai.com/

Clarifai aims to produce a more general recognition system that can be tailored for specific use cases. They want their customers to build their own model to implement the API, so the results are more specialized. It can help with the **organization** of images by analyzing a photo, identifying nuances and tagging it accordingly, and then using those tags to categorize. **Moderation** of a platform can also be streamlined by finding a pattern, and then eliminating submissions that deviate from the pattern. This type of technology also makes visual search possible. If parameters of an images can be discerned, then a user can use one image to search for similar results. This feature was added to google search in 2011, and revolutionized the way the general public queried the internet.



Custom
Create your own model and teach it with your own images and concepts

Apparel
Recognize clothing, accessories, and other fashion-related items

Celebrity
Identify celebrities that closely resemble detected faces

Color
Identify the dominant colors present in your media in hex or W3C form

Demographics
Predict the age, gender, and cultural appearance of detected faces

Face Detection
Detect the presence and location of human faces with a bounding box

Focus
Returns overall focus score and identifies in-focus regions within an image

Food
Recognize food items and dishes, down to the ingredient level

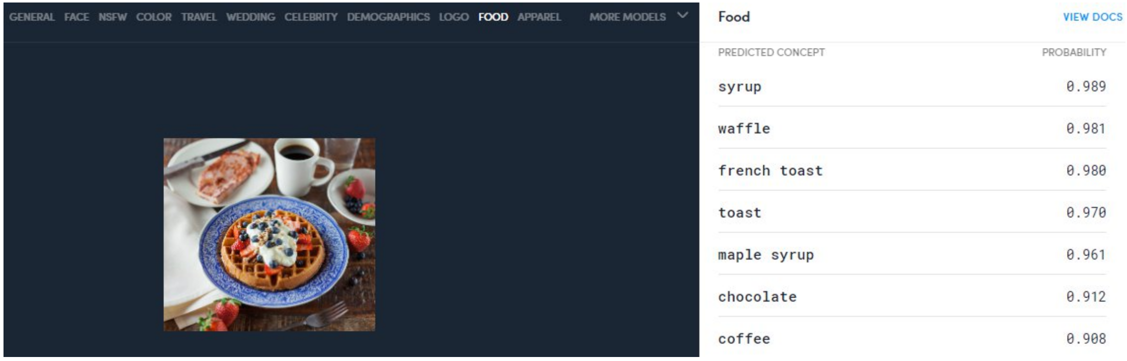
General
Our most comprehensive model with concepts, objects, scenes, and more

General Embedding
Computes numerical embedding vectors using our 'General' model

Logo
Detect and identify brand logos within images

NSFW
Identify different levels of nudity in visual content

The models that Clarifai suggest show various intriguing ways to pull relevant information from an image. The general model simply scans for shapes, objects, people, and other components. It then compiles a list of terms that describe the picture. However, the client can adjust the default analysis settings to tailor the scan for their industry/use case. Clarifai offers various sample models in the demo app. For example, if you select the 'demographic' model, it first determines if there are people in the photo. Then, the gender, age, and nationality of the subjects are calculated with a probability of correctness displayed. These identifiers change with each model. The 'nsfw' model simply rates the explicit content of the image and gives a probability that the image is not suitable for work. The 'food' model focuses more on searching for various components of a meal, and returns individual food items in a list. A gourmet food blog photographer would find this tool extremely useful to categorize the thousands of pictures they have from various restaurants.



Food

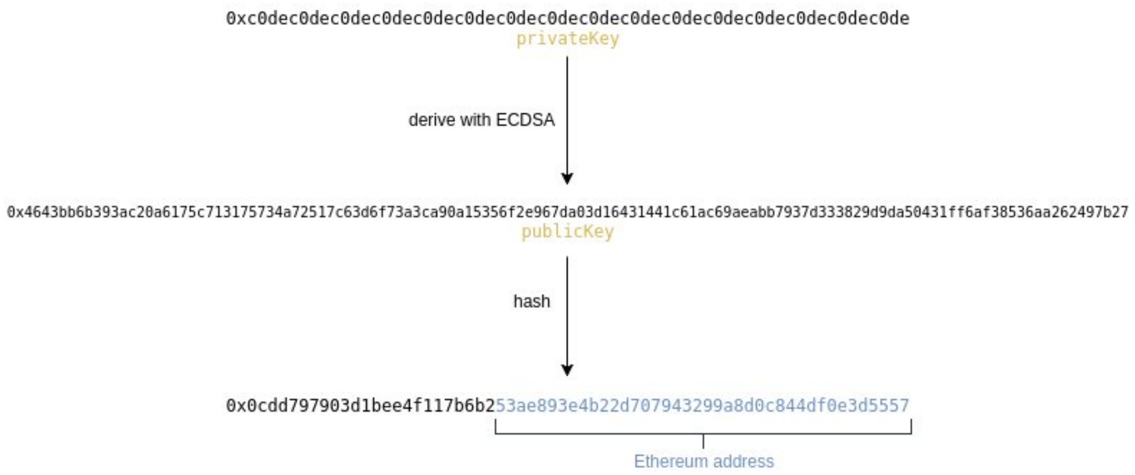
PREDICTED CONCEPT	PROBABILITY
syrup	0.989
waffle	0.981
french toast	0.980
toast	0.970
maple syrup	0.961
chocolate	0.912
coffee	0.908

Microsoft Vision API

Computer Generated Faces as “QR Codes” for Ethereum Public Keys

Ethereum Public/Private Key Cryptography Overview

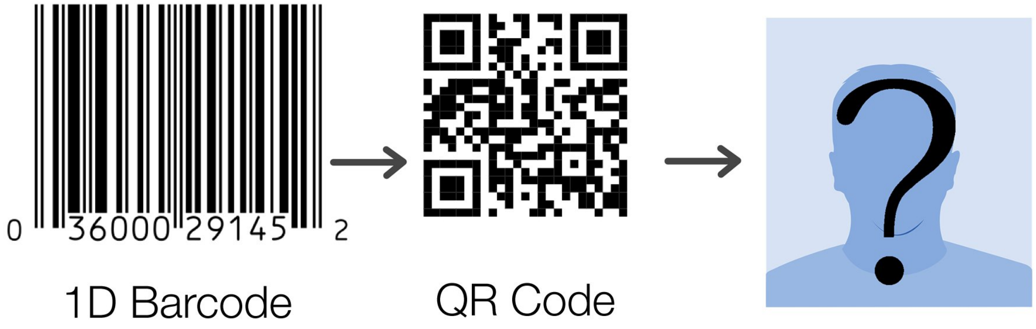
Ethereum uses a system known as public/private key cryptography to sign and verify data transacted throughout the blockchain. The private key is any 256-bit blob, with a few restrictions (e,g., cannot be all zeros). Using the **Elliptic Curve Digital Signature Algorithm (ECDSA)** with **sec256k1**, one can derive the public key from the private key. Taken one step further, when the public key is hashed using **SHA3-256 (Keccak)** function, the last 160 bits of the result are the Ethereum address. Therefore, all three critical pieces of information (public key, private key, and address) are all related mathematically. Every Ethereum address technically “pre-exists”, it is simply up to someone to locate the corresponding keys.


0xc0dec0dec0dec0dec0dec0dec0dec0dec0dec0dec0dec0dec0dec0dec0dec0de
privateKey
derive with ECDSA
0x4643bb6b393ac20a6175c713175734a72517c63d6f73a3ca90a15356f2e967da03d16431441c61ac69aeabb7937d333829d9da50431ff6af38536aa262497b27
publicKey
hash
0x0cdd797903d1bee4f117b6b253ae893e4b22d707943299a8d0c844df0e3d5557
Ethereum address

The public key is an extremely long and complicated string of characters. It would be a significant undertaking to attempt to memorize a public key, as it has no patterns or template.

How can we make the public key recognizable, relatable, and maybe even fun??

Due to the shortcomings mentioned, QR codes have no place in Web 3.0. Just as the QR code vastly improved upon functionality established by the barcode, Ethereum should have it's own unique way of visually expressing complicated data.



Currently, uPort mimics the ergonomic UI design that was pioneered by Snapchat. The landing screen simply activates the mobile camera, with the implication that scanning something will be a primary function in the final product. This will allow the user to quickly add connections, credentials, and other verifications. However, currently we are relying on the outdated QR code technology to interact with the real world. The downsides to QR codes have already been discussed at length, and are significant enough to warrant considering an alternative solution.

Humans recognize facial features more than any other visual cue in existence. We can identify our friend from across a busy intersection. We tell people that they look like certain celebrities because it is so easy for a face to feel familiar. It is an instantaneous recognition when you realize that a child looks like their parents. Faces are such an integral part to human identity, it's only right that it should be factored into a self-sovereign, digital identity.