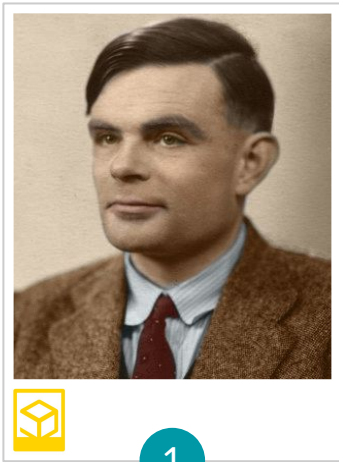
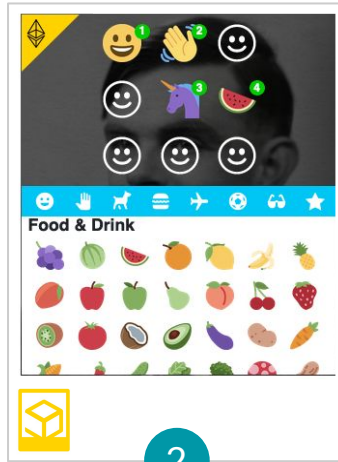


How PhotoKey Works



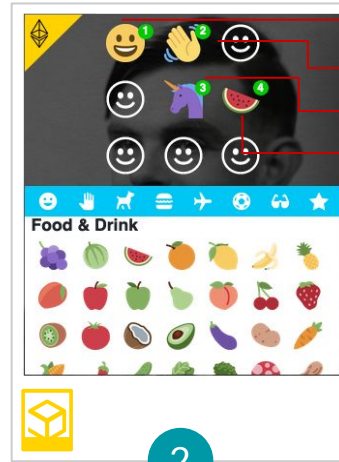
1

User uploads their photo



2

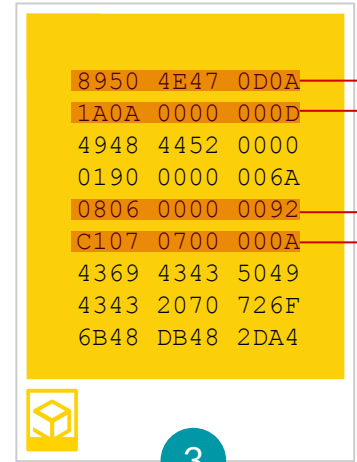
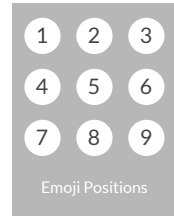
User creates EmojiKey by choosing emojis at each of nine positions in sequence.



2

PhotoKey gets the byte value for each emoji in sequence, ignoring empty positions.

- (1) 1F600
- (2) 1F44B
- (3) 1F984
- (4) 1F349



3

PhotoKey divides photo bytes into nine segments and extracts bytes for each emoji position.

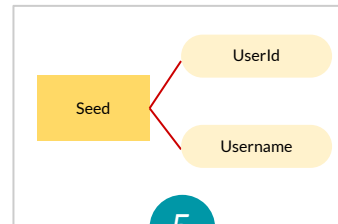
- 8950 4E47 0D0A (1)
- 1A0A 0000 000D (2)
- 4948 4452 0000
- 0190 0000 006A
- 0806 0000 0092 (5)
- C107 0700 000A (6)
- 4369 4343 5049
- 4343 2070 726F
- 6B48 DB48 2DA4

```
H1 = blake2s("1F600", "89504E470D0A")
H2 = blake2s("1F44B", "1A0A0000000D")
H3 = blake2s("1F984", "080600000092")
H4 = blake2s("1F349", "C1070700000A")

Seed = blake2s(H1, H2, H3, H4)
```

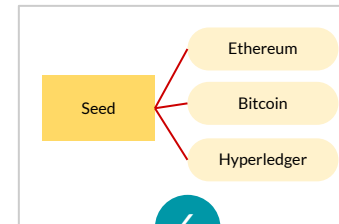
4

PhotoKey uses the Blake2s algorithm to hash emoji bytes with photo bytes for each position, and finally, produces an aggregate hash of the positional hashes. This is the high-entropy seed for keygen.



5

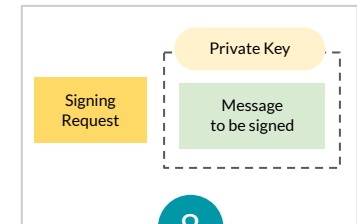
The seed is used to deterministically generate a UserId and Username in "adjective - phonetic word" format. Their hash is compared to the hash stored in the XMP (eXtensible Metadata Platform) photo section.



6

If the hash matches, the same seed is used to deterministically generate a public key and account address for the blockchain where PhotoKey is being used.

No private key or any other security information is ever stored in PhotoKey!



8

The public key and account address are reported to the calling application. The private key is only generated for signing requests and not available to the application.

Current Context

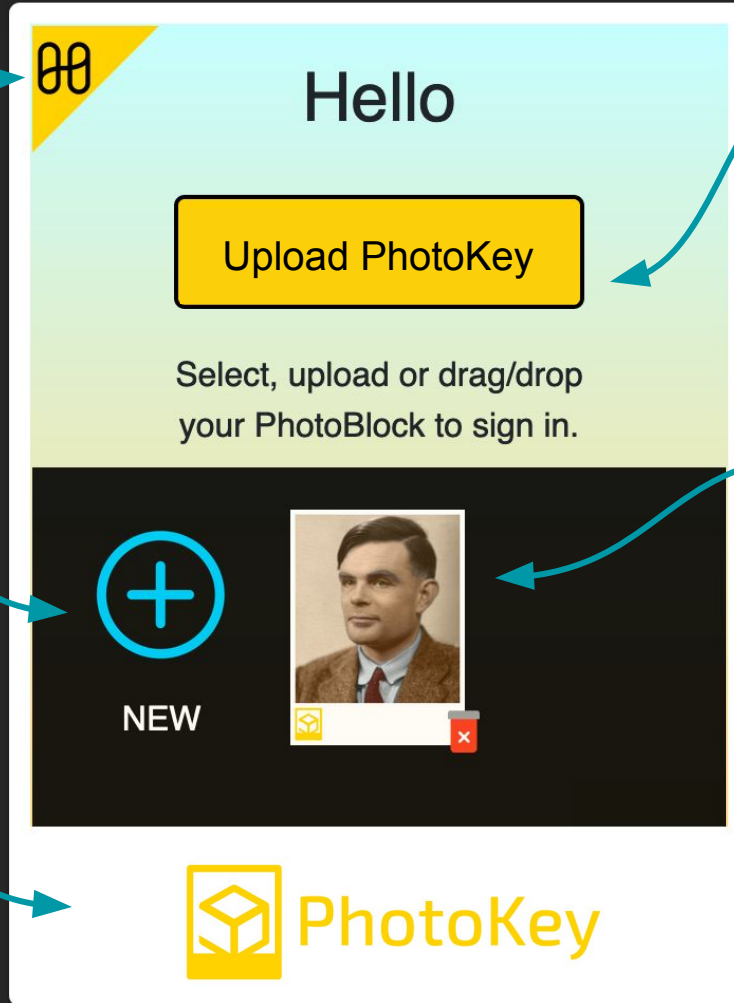
Indicates the blockchain that is currently in use with PhotoKey.

New PhotoKey

Enables the user to upload any JPEG photo that is then transformed into a PhotoKey.

Polaroid Frame

Overall look-and-feel of a familiar Polaroid instant photo.



Sign In

User uploads or drags an existing PhotoKey to sign in. This is for first-time use since once a PhotoKey is used it is available in recents.

Recent PhotoKeys

Recently used PhotoKeys are automatically persisted in the browser's IndexedDb storage. Browser security policy prevents access to the storage from any location other than the URL where it was created. When using the default PhotoKey service, this will be auth.photokey.org.