Cryptographic Proof Of Production

A very simple website with very big implications.

CPOP is a concept made possible by the recent(ish) introduction of BIP32 functionality into cryptocurrencies like Bitcoin.

For those not in the know, BIP32 is a standard by which it is possible to create a master private and public keys from which many 'babie' subkeys can be produced.

These subkeys are mathematically linked to one another so for example Bitcoins can be sent to a sub public key address generated by Alice who lives in the UK using the master public key but the funds can only be spent by Bob who lives in America and has the master private key.

This is clearly very useful but what else can we do with this?
We can use it for identification!

Our idea is simple, businesses (and individual people if they wish) can register their master public key with our website which members of the public will be able to visit and confirm if the public key provided to them belongs to the company/individual they believe it does.

An example use case:
Alice buys some medication from a website she has never used before.
When the medication arrives she opens the bottle and takes out a pill which is imprinted with a unique public key, she can then submit the key to our site and if the pharmaceutical company has registered their master public key with us we will be able to tell Alice who the producer of the medication was and how many times that unique key has been submitted to our site in the past.
If Alice sees that she is indeed the first person ever to submit the key and the producer of the key matches the producer of the medication she can take the pill with confidence.
If however she sees that the key is not registered to the producer claimed or that the key has been submitted before then she will know that the pill is a fake and avoid a potentially dangerous situation.

This technology could potentially save lives.

Other use cases include protection against the forgery of goods such as clothing and accessories, the importance of which will likely rise over time as 3D printed products become more and more proliferant.
Companies whose products are purchased using cryptocurrency may even choose to imprint the product with the key to which the customer paid so that the item can then be verified and a record of the date, time and amount paid will always be available.

Another feature of this method is 'blockchain unburdening', the scanning and submitting of keys in this way does not involve the blockchain and will not contribute to any unnecessary bloat.

Bullets, condoms, electronic parts, the list is endless.

A prototype is available for testing at http://cryptoproof.info