Suppose a customer wants a bank to sign a piece of digital cash with the serial number x, but does not want the bank to know which piece of cash it is signing. Basically you want keep your anonymity but still get the endorse of the validity from the bank. This can be achieved with a blind signature protocol.

1. Customer chooses a random number r, and send $xr^e \pmod N$ where e and N are bank's public keys.
2. Bank signs the digital cash with private key d:

$$(xr^e)^d \equiv x^d r^{ed} \equiv rx^d \pmod N$$

   (Recall in the proof of RSA, $x^e d \equiv x \pmod N$, so $r^e d \equiv r \pmod N$)

3. Then bank sends back the result to customer.
4. The customer divides out the blinding factor to get bank's signiture:

$$(rx^d)r^{-1} = x^d \pmod n$$

   .

Basically, for later use, customer can just send the signed digital cash $x^d \pmod n$ to the bank. And only the bank can verify it later.