News

1. Developer Survey https://insights.stackoverflow.com/survey/2019
2. Worlds 2nd largest food retailer, Albersons, joins IBM Food Trust.
3. Coinbase now provides a VISA card so you can spend your crypto.

Zero Knowledge Identification System

Paper: https://arrow.dit.ie/cgi/viewcontent.cgi?article=1031&context=itbj

Look at page 38, section 7.9. to 7.12 on page 43.

Walk through of algorithm with the example from the paper.

Also see: https://blog.cryptographyengineering.com/2017/01/21/zero-knowledge-proofs-an-illustrated-primer-part-2/

Zero knowledge proof for use as ID

```
package main

import (
        "crypto/rand"
        "fmt"
        "math/big"
        "os"
)

// From: https://arrow.dit.ie/cgi/viewcontent.cgi?article=1031&context=itbj
// IdProtocalsInCrypto.pdf -- See p. 38, 40, 41

func main() {
        // From p40
        p := big.NewInt(88667)
        q := big.NewInt(1031)
        alpha := big.NewInt(70322)
        a := big.NewInt(755)

        // v = (alpha ^ ( q-a )) % p
        t1 := big.NewInt(0)
        t1.Sub(q, a)
```

```
v := big.NewInt(0)
v.Exp(alpha, t1, p)

fmt.Printf("Setup Complete: v=%s\n", v)

// Alice is the Client:

// ------------------------------------------------------------
// Message 1 - Client to Server
// ------------------------------------------------------------

// Alice Chooses, and send to Bob
// r := big.NewInt(543) // Should be random, but for this example
M := big.NewInt(9999) // Generate crypto random value
r, err := rand.Int(rand.Reader, M)
if err != nil {
        fmt.Printf("Failed to generate random value, %s\n", err)
        os.Exit(1)
}
x := big.NewInt(0)
x.Exp(alpha, r, p) // x=(alpha^r) % p

fmt.Printf("Send To Bob : x=%s\n", x)

// ------------------------------------------------------------------------
// Response to Message 1, Server back to client
// ------------------------------------------------------------------------

// Bob is the Server:
// Bob sends the challenge 'e' back to Alice e to do the computation
// e = 1000

// Alice now computes: y = a*e % q

// ADD CODE -

fmt.Printf("y=%s\n", y) // Prints 851

// ------------------------------------------------------------------------
// Message 2 - Client (Alice) with response to challenge.
// ------------------------------------------------------------------------

// Bob (server) verifies: x == z == (a^y) * (v^e) % p
// Bob (server) verifies: x == z == ((a^y)%p)*((v^e)%p) % p

// ADD CODE -

fmt.Printf("z=%s\n", z)

// ------------------------------------------------------------------------
// Response 2 - Success/Fail message from server back to client
```

```
        // ------------------------------------------------------------------------
        if x.Cmp(z) == 0 {
                fmt.Printf("Authoized! Yea\n")
        } else {
                fmt.Printf("Nope nope nope\n")
        }

}
```