$\mathcal{B}$	Bank
$\mathcal{U}$	User
$\mathcal{S}$	Shop
(g, g_1, g_2)	Erzeugertupel von G_q
$x \in \mathbb{Z}_q$	privater Schlüssel der Bank
$h=g^x$	öffentlicher Schlüssel der Bank
$\mathcal{H}$: Gq × Gq × Gq × Gq × Gq → $\mathbb{Z}_q^*$	kollisionsresistente Hashfunktion (Abheben)
u_1	Zufallszahl auf User registriert
$I = g_1^{u_1}$	Identität des Users
$m = Ig_2 = g_1^{u_1} g_2^1$	Message im Grunde die Münze
$z = (Ig_2)^x$	
w, s, x_1, x_2, u, v	Zufallszahlen
$a = g^w$	
$b = m^w = (Ig_2)^w$	
$A = (Ig_2)^s = m^s$	geblendete Message
$B = g_1^{x_1} g_2^{x_2}$	
$A, B, sign(A,B)$	Münze
$\mathcal{H}_0 : G_q \times G_q \times \text{Shop-ID} \times \text{Datum/Zeit} \rightarrow \mathbb{Z}_q$	kollisionsresistene Hashfunktion (Bezahlen)