



Trabajo Practico: \$BerretaCoin

Cómo funcionan las transacciones dentro de las Blockchains

6 de abril de 2025

Algoritmos y Estructura de Datos

Grupo 30

Integrante	LU	Correo electrónico
Rankov, Jorge	714/23	jrankov@dc.uba.ar
Falbo, Tiziana	nnn/nn	nnn@gmail.com
Facundo	nnn/nn	nnn@gmail.com
Bautista	nnn/nn	nnn@gmail.com



Facultad de Ciencias Exactas y Naturales
Universidad de Buenos Aires

Ciudad Universitaria - (Pabellon I/Planta Baja)

Intendente Guiraldes 2610 - C1428EGA

Ciudad Autónoma de Buenos Aires - Rep. Argentina

Tel/Fax: (+54 +11) 4576-3300

<http://www.exactas.uba.ar>

TAD \$BerretaCoin {

obs bc: Seq<Seq< $\mathbb{Z} \times \mathbb{Z} \times \mathbb{Z} \times \mathbb{Z}$ >>

proc agregarBloque (inout bc: \$BerretaCoin; in bloque: Seq< $\mathbb{Z} \times \mathbb{Z} \times \mathbb{Z} \times \mathbb{Z}$ >){
requiere{ ($|bc| < 3000$) \wedge_L ($|bloque| < 50$) }
requiere{ esTransaccionCreacion(bloque_[0]) }
requiere{ ($\forall i: \mathbb{N}$) ($0 \leq i < |monto| \rightarrow_L$ (bloque_{[i][1]} \neq bloque_{[i][2]})) }
asegura{ (\exists idMontos: Seq< $\mathbb{Z} \times \mathbb{Z}$ >)(sinRepetirId(idMontos) \wedge_L
esTransaccionValida(bloque, idMontos)) }
asegura{ bc = concat(bc₀) }
asegura{ $|bc| = |bc_0| + 1$ }
}

proc montosDeUsuarios {
asegura: $\forall id \in \text{sinRepetidos}(\text{Usuarios}(\text{Cripto.blockchain})) \rightarrow id \in \text{res}$
 \longleftrightarrow (esMaximo(MontoUsuario(Cripto.blockchain, id));
Montos(Usuarios(Cripto.blockchain)))
}

pred esTransaccionCreacion (t: Seq< $\mathbb{Z} \times \mathbb{Z} \times \mathbb{Z} \times \mathbb{Z}$ >) {
 $t_{[1]} = 0$
}

pred sinRepetirId (ids: Seq< $\mathbb{Z} \times \mathbb{Z}$ >) {
($\forall i, j: \mathbb{N}$) (($0 \leq i < |ids| \wedge_L$ ($0 \leq j < |ids| \wedge_L$ ($j \neq i$))
 \rightarrow_L id_{[i][0]} \neq id_{[j][0]}))
}

pred esMaximo (Monto: \mathbb{Z} , Montos: Seq< \mathbb{Z} >) {
($\forall i \in \text{Montos}$) \rightarrow_L Monto $\geq i$
}

proc montoMedio (S: Seq<Seq< $\mathbb{Z} \times \mathbb{Z} \times \mathbb{Z} \times \mathbb{Z}$ >>): \mathbb{Z} {
requiere: \forall bloque $\in S$, $|bloque| > 0$

$$\text{asegura: res} = \frac{\sum_{j=0}^{|S|-1} \sum_{i=1}^{|S[j]|-1} S_{[j][i][3]}}{\sum_{j=0}^{|S|-1} (|S[j]|-1)}$$

}

pred esTransaccionValida (b: Seq< $\mathbb{Z} \times \mathbb{Z} \times \mathbb{Z} \times \mathbb{Z}$ >, ids: Seq< $\mathbb{Z} \times \mathbb{Z}$ >) {
 $(\forall i, j: \mathbb{N}) (j \leq i < |b| \wedge_L (0 \leq j < |ids|) \wedge_L (b_{[i][2]} = ids_{[j][0]})$
 $\rightarrow_L (b_{[i][3]} \leq ids_{[j][1]})$
}

aux sinRepetidos(S: Seq< \mathbb{Z} >): Seq< \mathbb{Z} >=

$$[S_{[0]}] + \sum_{i=1}^{|s|-1} ifThenElse(S_{[i]} \in SubSeq(S, 0, i-1); \emptyset; [S_{[i]}])$$

aux Usuarios(S: Seq<Seq< $\mathbb{Z} \times \mathbb{Z} \times \mathbb{Z} \times \mathbb{Z}$ >>): Seq< \mathbb{Z} >=

$$\sum_{i=0}^{|s|-i} \sum_{j=0}^{|s_{[i]}|-1} (S_{[i][j][1]}, S_{[i][j][2]})$$

aux MontoUsuario (S: Seq<Seq< $\mathbb{Z} \times \mathbb{Z} \times \mathbb{Z} \times \mathbb{Z}$ >>; id: \mathbb{Z}): \mathbb{Z} =

$$\sum_{j=0}^{|s|-1} \left(\sum_{i=0}^{|s_{[j]}|-1} ifThenElse(id = S_{[j][i][1]}; S_{[j][i][3]}, 0) - \sum_{j=0}^{|s|-1} ifThenElse(id = S_{[j][i][2]}; S_{[j][i][3]}, 0) \right)$$

aux Montos (S: Seq< \mathbb{Z} >): Seq< \mathbb{Z} >=

$$\sum_{j=0}^{|s|-1} (MontoUsuario(S_{[i]}))$$

}