DEPARTAMENTO
DE COMPUTACION
Facultad de Ciencias Exactas y Naturales - UBA

Trabajo Practico: $BerretaCoin

Cómo funcionan las transacciones dentro de las Blockchains

April 11, 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 blockchain: 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{ $(|bc| < 3000) \land_L (|bloque| < 50)$ }

requiere{ esTransaccionCreacion (bloque$_{[0]}$) }

requiere{ (∀i: $\mathbb{N}$) (0 ≤ i < $|bloque|$ $\rightarrow_L$ (bloque$_{[i][1]}$ ≠ bloque$_{[i][2]}$)) }

asegura{(∃ idMontos: Seq<$\mathbb{Z}\times\mathbb{Z}$>) (sinRepetirId (idMontos)
$\land_L$ esTransaccionValida (bloque, idMontos))}

asegura{ bc = concat (bc$_0$, <bloque>) }

asegura{ |bc| = |bc$_0$|+1 }

}

proc agregarBloque2.0 (inout BC.Berret, S:Seq<$\mathbb{Z}\times\mathbb{Z}\times\mathbb{Z}\times\mathbb{Z}$>) {

requiere { $B = B_0 \land 0 < |s| \leq S_0 \land bloqueValido(BC, S)$ }

asegura { bc.blockchain = 0 b$_0$.blockchain ++ S }

}

proc agregarBloque3.0 (inout cripto: BerretaCoin, in bloque:Seq<$\mathbb{Z}\times\mathbb{Z}\times\mathbb{Z}\times\mathbb{Z}$>){

requiere { length (cripto.blockchain) < 50 }

requiere { cripto = cripto$_0$ }

asegura { cripto.blockchain = concat (cripto$_0$.blockchain, <bloque>) }

}

proc montosDeUsuarios {

asegura { ∀id ∈ sinRepetidos (Usuarios (Cripto.blockchain)) → id ∈ res
$\longleftrightarrow$ (esMaximo (MontoDeUsuario (Cripto.blockchain, id));
Montos (Usuarios (Cripto.blockchain))) }

}

proc maximosTenedores (in bc: BerretaCoin): Seq<$\mathbb{Z}$> {
asegura { ($\forall$i: $\mathbb{Z}$)($0 \leq i < |res|$) $\rightarrow$ esUsuario ($res_{[i]}$, bc.blockchain) }

asegura { ($\forall$id: $\mathbb{Z}$) (id $\in$ res) $\longleftrightarrow$
$\neg$ ($\exists$ otro: $\mathbb{Z}$) (esUsuario (otro; bc.blockchain))
$\wedge$ (montoDeUsuario (otro, bc) $\geq$ MontoDeUsuario (id, bc)) }
}

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

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

proc Usuarios (in bc: BerretaCoin): Seq<$\mathbb{Z}$>{
asegura{ ($\forall$i: $\mathbb{Z}$) ($0 \leq i < |bc.blockchain|$)}

asegura{ ($\forall$j: $\mathbb{Z}$) ($0 \leq i < |bc.blockchain_{[i]}|$)}

asegura{($bc.blockchain_{[i][j][1]} \wedge bc.blockchain_{[i][j][2]}$) $\in res$
$\wedge$ ningunOtroElem $\in res$ }
}

Predicados

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

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

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

pred esUsuario (id: $\mathbb{Z}$, b: Seq$<$Seq$<\mathbb{Z}\times\mathbb{Z}\times\mathbb{Z}\times\mathbb{Z}>>$) {
$\quad (\exists \mathrm{i}\colon \mathbb{Z})\ (\exists \mathrm{j}\colon \mathbb{Z})\ (0 \leq \mathrm{i} < |b| \wedge_L 0 \leq \mathrm{j} < |b_{[i]}|) \wedge$
$\qquad (\mathrm{id} = \mathrm{b}_{[i][j]_{[1]}} \vee \mathrm{id} = \mathrm{b}_{[i][j]_{[2]}})$
}

pred bloqueValido (B: Seq$<$Seq$<\mathbb{Z}\times\mathbb{Z}\times\mathbb{Z}\times\mathbb{Z}>>$, S: Seq$<\mathbb{Z}\times\mathbb{Z}\times\mathbb{Z}\times\mathbb{Z}>$){
$\quad (|\mathrm{B}| < 3000 \rightarrow \mathrm{S}_{[0]_1} = 0) \wedge (|\mathrm{B}| > 3000 \rightarrow \mathrm{S}_{[0]_1} \neq 0) \wedge (0 < |S| \leq 50)$
}

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

1 Auxiliares

aux sinRepetidos (S: Seq<ℤ>): Seq<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<ℤ×ℤ×ℤ×ℤ>>): Seq<ℤ>=

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

aux MontoDeUsuario (id:ℤ; B:BerretaCoin): ℤ=

$$\begin{aligned}\sum_{i=0}^{|b.blockchain|-1} & -\left(\sum_{j=0}^{|b.blockchain_{[i]}|-1} ifThenElse(id = b.blockchain_{[i][j]_1}, b.blockchain_{[i][j]_3}, 0)\right) \\ & + \left(\sum_{j=0}^{|b.blockchain_{[i]}|-1} ifThenElse(id = b.blockchain_{[i][j]_1}, b.blockchain_{[i][j]_2}, 0)\right)\end{aligned}$$

aux Montos (S: Seq<ℤ>): Seq<ℤ>=

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

}