計算用紙

まい月

はじめに

　本書は著者が試してみたいと思うことをリストするという体でLaTeXとTikZを練習する文書である。

目次

第1章
ステーブルコインのようなもの

1.1 状況

ブロックチェーンで流通するトークン🍑を裏付けとして、ある価値🍎と連動したトークン🍃を発行したい。

1.2 ためしてみたい解決策

参加者の財産	DAOの財産	レバレッジ	🍃/🍑
• 現物1000🍑	0	0.5倍	1🍑
参加者は1000🍑を担保に10🍃鋳造する			
• 1000🍑を担保に10🍃鋳造したポジション • 現物10🍃	• 現物1000🍑	0.5倍	1🍑

Table 1.1: 鋳造する手続き

参加者の財産	DAOの財産	レバレッジ	🍃/🍑
• 1000🍑を担保に10🍃鋳造したポジション • 現物10🍃	• 現物1000🍑	0.5倍	1🍑
参加者は10🍃焚いて1000🍑を返してもらう			
• 現物1000🍑	0	0.5倍	1🍑

Table 1.2: 焚く手続き

参加者 の財産	DAO の財産	レバ レッジ	🍃/🍑
• 1000🍑を担保に 10🍃鋳造した ポジション • 現物10🍃	• 現物1000🍑	0.5倍	1🍑
1🍃の価格が100🍑になり、 1000🍑にレバレッジの0.5倍を乗じた額を超えて 🍃を鋳造している状態になり強制ロスカする			
• 現物10🍃	• 現物1000🍑	0.5倍	100🍑

Table 1.3: 強制決済

第2章
インポータンスの計算の効率化

2.1 目標と方針

この節は理想についての演説にほかならず中身がない。

まずSymbolやNEMではブロックを検証するのに所定の条件を満たした適格なアカウントであることを要求していた。これは検証するための抽選とは別に、その抽選に参加するために必要なものであった。

そこでSymbolのPoS+を参考にしつつSymbolのPoS+より計算の効率と開かれ具合をすっごく上げたいと考えて。特にSymbolで採用されているPoS+と今回やりたいことの違いは：

- 所持金の下限を撤廃
  - ブロックチェーンに載っていれば適格
- ブロック毎に計算できる効率
- 毎回すべての適格なアカウントのインポータンスを計算しなくていい

であり、そのための原材料は：

- 残高
- 検証したブロックの数
- 支払った手数料

であり、ここまではSymbolと同じで、ここからが肝心なところで、これらすべての適格なアカウントについての総和がブロックヘッダに残ること、そしてこれがいたって自然な活動であれば尚良い。

2.2 準備

ブロックiごと	アカウント$j \in \mathcal{A}$ごと	パラメータ
• アカウントの数$\#\mathcal{A}$ • 総供給量$S_1(i)$ • ブロックの高さ$S_2(i)$ • 手数料の合計$S_3(i)$	• 残高$s_1(i,j)$ • 検証した回数$s_2(i,j)$ • 手数料の合計$s_3(i,j)$	• 遡るブロックH • ハッシュの大きさN • 理想の間隔T • 重み$\alpha_1, \alpha_2, \alpha_3$

Table 2.1: オンチェーンの情報

Table2.1のとおりブロックチェーンに書き込むものとして、色々計算する。

2.3 計算

そしてみんなここにしか興味なしであろう計算の部分です。

$$
\begin{aligned}
s\left(i,j\right) &\coloneqq \sum_{k=0}^{3} \alpha_k s_k\left(i,j\right) \\
S\left(i\right) &\coloneqq \sum_{k=0}^{3} \alpha_k S_k\left(i\right) \\
&= \sum_{j\in\mathcal{A}} s\left(i,j\right) \\
\tilde{I}\left(i,j\right) &\coloneqq \frac{\sum_{h=0}^{\min\{H,i\}-1} s\left(h,j\right)}{\sum_{h=0}^{\min\{H,i\}-1} S\left(h\right)} \\
M &\coloneqq NH\#\mathcal{A}+1 \\
I\left(i,j\right) &\coloneqq \frac{1}{M}\left\lfloor M\tilde{I}\left(i,j\right)\right\rfloor
\end{aligned}
$$

この$I\left(i,j\right)$、あるいはお好みの方法で減衰させたもの（e.g., $\tilde{I}\left(i,j\right)$の代わりに$\frac{\sum_{h=0}^{\min\{H,i\}-1}\gamma^{i-h}s\left(h,j\right)}{\sum_{h=0}^{\min\{H,i\}-1}\gamma^{i-h}S\left(h\right)}$（$\gamma\in\mathbb{Q}\cap(0,1)$）を使う、すると適当な$M$も変わりうる）をインポータンスとして使いたい。

2.4 導出過程

この節では、みんな興味ないかもしれないけど、$M\coloneqq NH\#\mathcal{A}+1$とする理由を説明する。$\forall i=1,2,\ldots;\left|1-\sum_{j\in\mathcal{A}} I\left(i,j\right)\right|<\frac{1}{N}$を満たせばよいから、

$$
\begin{aligned}
&\forall i=1,2,\ldots; \\
&\left|1-\sum_{j\in\mathcal{A}} I\left(i,j\right)\right|<\frac{1}{N}
\end{aligned}
$$

$$
\begin{aligned}
&\Leftrightarrow \left| \sum_{j\in\mathcal{A}} \left(\frac{\sum_{h=0}^{\min\{H,i\}-1} s(i,h)}{\sum_{h=0}^{\min\{H,i\}-1} S(h)} - \frac{1}{M} \left\lfloor M \frac{\sum_{h=0}^{\min\{H,i\}-1} s(i,h)}{\sum_{h=0}^{\min\{H,i\}-1} S(h)} \right\rfloor \right) \right| < \frac{1}{N} \\
&\Leftrightarrow \sum_{j\in\mathcal{A}} \left(\frac{\sum_{h=0}^{\min\{H,i\}-1} s(i,h)}{\sum_{h=0}^{\min\{H,i\}-1} S(h)} - \frac{1}{M} \left\lfloor M \frac{\sum_{h=0}^{\min\{H,i\}-1} s(i,h)}{\sum_{h=0}^{\min\{H,i\}-1} S(h)} \right\rfloor \right) < \frac{1}{N} \\
&\Leftarrow \sum_{j\in\mathcal{A}} \sum_{h=0}^{\min\{H,i\}-1} \left(\frac{s(h,j)}{\sum_{g=0}^{\min\{H,i\}-1} S(g)} - \frac{1}{M} \left\lfloor M \frac{s(h,j)}{\sum_{g=0}^{\min\{H,i\}-1} S(g)} \right\rfloor \right) < \frac{1}{N} \\
&\Leftarrow \sum_{j\in\mathcal{A}} \sum_{h=0}^{\min\{H,i\}-1} \frac{1}{M} < \frac{1}{N} \\
&\Leftarrow \frac{1}{M} H\#\mathcal{A} < \frac{1}{N} \\
&\Leftrightarrow NH\#\mathcal{A} < M \\
&\Leftarrow NH\#\mathcal{A} + 1 = M.
\end{aligned}
$$

例えば、ハッシュにはKeccak512を用い、アカウントは1000こあり、ブロックは300000ブロック前まで遡って良いものとして、$M = 2^{512} \cdot 300000 \cdot 1000 + 1$となる。