Метод усечения блокчейна в пространстве состояний

noise@sumus.team

1 ноября 2018 г.

Аннотация

Предлагается системный подход к процессу усечения блокчейна, основанный на теории пространства состояний динамической системы. Рассматривается усечение блокчейна двух видов: по времени, что позволяет условно "отбросить" предысторию системы и по фазовым координатам, что позволяет уменьшить размерность пространства состояний на некотором интервале времени.

1 Введение

При длительной истории (отдельно взятой) конкретной истории блокчейн и большом количестве узлов рано или поздно возникает проблема вычислительных ресурсов, связанная с необходимостью поддерживать в постоянной готовности к доступу всю информацию, накопленную за всю историю и обо всех сущностях системы, включая "обнулившиеся" кошельки, "спящие" узлы и тому подобное. Даже при высоких возможностях современных компьютерных систем это приводит к появлению некоторого "балласта", на поддержание информации о котором в постоянной готовности тратятся значительные ресурсы. Для решения данной проблемы предлагается процедура "усечения" блокчейна, позволяющая отбросить неактуальные фрагменты, но и сохранить "прозрачность" системы для пользователей и полную преемственность информации. Для достижения этой цели предлагается использовать описание блокчейна как системы в пространстве состояний.

2 Основные положения и допущения

Пусть задано n-мерное линейное метрическое пространство $\mathbb{X}$ с метрикой $\rho(x_1, x_2)$, где $x_1, x_2 \in \mathbb{X}$. Пусть оно является пространством состояний системы S, состоящей их r линейнозависимых элементов S_l, $l = 1, \ldots, r$, каждый из которых может быть представлен точкой подпространства $\mathbb{X}_l, \dim \mathbb{X}_l = k_l$ пространства $\mathbb{X}, \sum_{l=1}^{r} k_l = n$. В этом случае состояние системы S в момент времени t может быть представлено точкой $A(x_1, \ldots, x_n)$ пространства $\mathbb{X}$, причём радиус-вектор $\vec{a}$ этой точки является блочным вектором $\vec{a} = (x_{11}, \ldots, x_{1k_1}|x_{21}, \ldots, x_{2k_2}|x_{r1}, \ldots, x_{rk_r})$, где каждый "блок" вектора соответствует "своему" подпространству.

Траекторией системы S будем называть кривую $\Gamma \subset \mathbb{X}$, начальная точка которой A_0 соответствует моменту времени t_0, конечная точка A_1 — t_1. Таким образом, траектория Γ соответствует отрезку $[t_0, t_1]$, а t является параметром, откладываемым вдоль кривой.

На рис. 1 изображена траектория системы S при $n = 3$, $r = 2$, $k_1 = 2$, $k_2 = 1$. Значение координаты $x_{ij} (1 \leq i \leq r; 1 \leq j \leq k_l, l = 1, \ldots, r)$ будем называть "ε_{ij}-нулевым", если при заданном малом ε_{ij}.

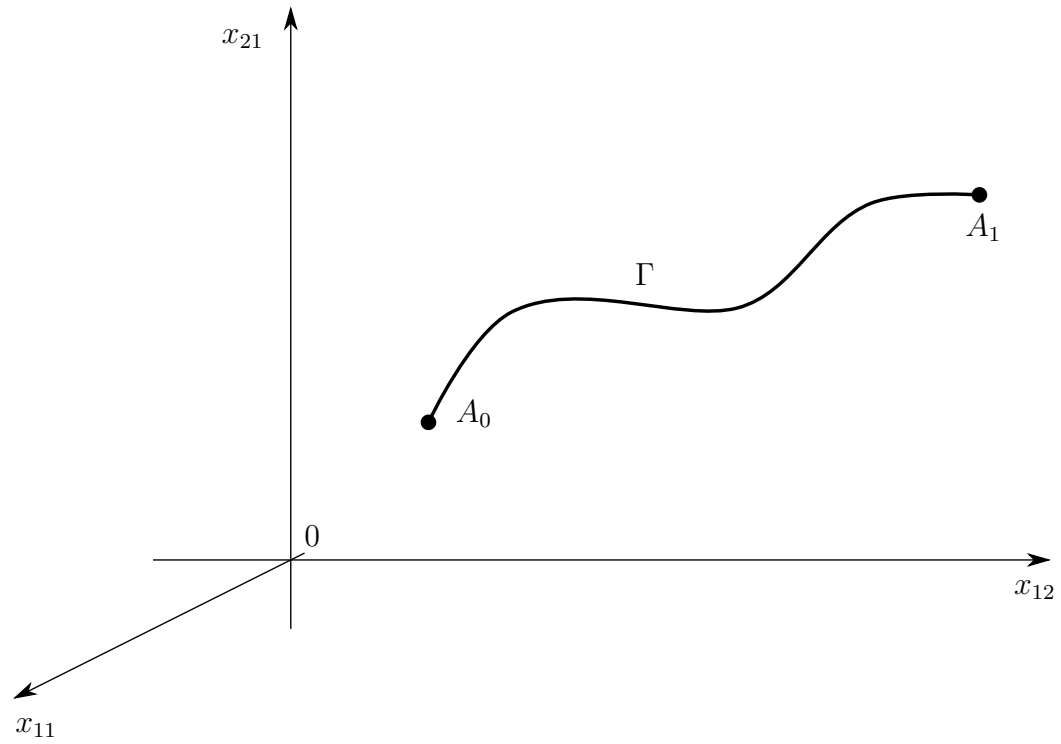

Рис. 1: Траектория системы S в пространстве $\mathbb{X}$.

$$|x_{ij}| \leq \varepsilon_{ij} \tag{1}$$

Если система S — блокчейн, то её элементы S_l есть: (а) узлы; (б) кошельки; (в) genesis-блок; (г) остальные блоки.

(а) отдельный узел, соответствующий элементу системы с номером i описывается следующими переменными:

- x_{i1} – отношение откликов узла на обращения системы на текущий момент к числу этих обращений.
- x_{i2} – суммарное вознаграждение ζ, выплаченное этому узлу на текущий момент.

Возможны и другие переменные состояния узла.

(б) переменной состояния кошелька j — номер этого кошелька как элемента системы - x_{j1} является сумма (количество) средств в нём на текущий момент в одной валюте. Если имеется k валют, то следующая переменная x_{jk+1} — это бинарная переменная, значения которой соответствуют способности кошелька открывать узлы: 0 - не способен, 1 -способен.

(в) Genesis (G-блок) имеет смысл назначить элементом системы номер 1. Тогда переменными состояния G-блока будут номера (адреса) корневых узлов, зарегистрированных в этом блоке: $x_{1i_1}, x_{1i_2}, \ldots, x_{1i_\nu}$. Также описываются другие корневые сущности. В совокупности их количество будет равно $k_{l_G} = \dim \mathbb{X}_{l_G}$.

(г) Остальные блоки включаются в "цепочку" и характеризуются одной переменной x_{mk_s} , значение которой равно в текущий момент времени количеству закрытых блоков в цепочке.

3 Виды усечения блокчейна

"Усечение" системы может быть I и II рода.

I. "Усечение" I рода есть "усечение" по времени. Исходя из анализа функционирования си-

стемы S, выбирается момент времени $t_0 < t^* < t$, такой, для которого координаты системы постоянны на интервале $[t^*, t^* + \delta]$, $\delta \ll t_2 - t_1$. Точка $A^* : (x^*_{11}, \ldots, x^*_{kk_l})$ в момент времени t^* объявляется новым начальным состоянием системы S. Для блокчейна в этот момент t^* все блоки закрыты, транзакции не производятся. В G-блоке все настройки остаются прежними (вообще говоря, считается, что до усечения все координаты G-блока остаются постоянными), т.е. движение системы на $[t_1, t^*]$ есть движение в некоторой гиперплоскости (линейном многообразии размерности $(n - k_{l_G})$, где l_G - номер подпространства G-блока). Вся предыстория системы S на интервале $[t_1, t^*)$ отбрасывается, но запоминается.
"Усечение" I рода возможно только тогда, когда система S является *вполне управляемой*. Это значит, что для $\forall$ двух точек пространства $\hat{A}, \tilde{A} \in \mathbb{X}$, существует такое управление (воздействие на блокчейн со стороны создателей), что S может быть переведена из точки $\hat{A}$ в точку $\tilde{A}$. Переход из $\hat{A}$ в $\tilde{A}$ считается успешным, если полностью восстановлены все координаты S в момент $\tilde{t}$, соответствующий $\tilde{A}$.
II. "Усечение" II рода есть "усечение" по фазовым координатам. Пусть в момент t^* q координат x_{ij} являются "ε_{ij}-нулевым" для μ нулевых блоков с номерами $l_1, \ldots, l_\mu$. Если принимается решение об "усечении" II рода, то эти q координат отбрасываются (с запоминанием) и движение системы S продолжается в пространстве $\mathbb{X}_{n-q} \subset \mathbb{X}$ ($\mathbb{X}_{n-q} \rhd \mathbb{X}$). При этом в момент t^* "скачком" меняются значения координат G-блока, но изменения размерности k_{l_G} подпространства $\mathbb{X}_{l_G}$ не происходит. Координаты G-блока меняются на числа равные номерам (адресам) сущностей, оставшихся в G-блоке после усечения. Размерность k_{l_G} меняется только в случае изменения количества корневых узлов.
Дальнейшее движение S (при $t > t^*$) может сопровождаться возрастанием размерности пространства состояний до n и более.

4 Пример усечения блокчейна

Пусть система S (блокчейн) состоит только из двух элементов $l = 1, 2$ $(r = 2)$. S_1 — G - блок. x_{11} — переменная, соответствующая адресу корневого узла, зарегистрированного в этом блоке. G - блоку соответствует подпространство $\mathbb{X}_1$, $\dim \mathbb{X}_1 = 1$. S_2 — кошелёк, где x_{21} — количество средств в этом кошельке в одной валюте, x_{22} — бинарная переменная, характеризующая способность кошелька создавать узлы: $x_{22} = 1$ — кошелёк способен открывать узлы; $x_{22} = 0$ — кошелёк не способен открывать узлы. Кошельку соответствует подпространство $\mathbb{X}_2$, $\dim \mathbb{X}_2 = 2$.

$$\mathbb{X} = \mathbb{X}_1 \times \mathbb{X}_2 \tag{2}$$

Переменные x_{11}, x_{22} принадлежат конечным или счётным множествам неотрицательных чисел. Переменную x_{21} будем считать принадлежащей множеству неотрицательных чисел.

Пусть заданы ε_{11}, ε_{22} – неотрицательные числа такие, что при выполнении неравенств:

$$|x_{11}| \le \varepsilon_{11} \; ; \;\; (x_{11} \le \varepsilon_{11}) \; ; \;\; |x_{22}| \le \varepsilon_{22} \; ; \;\; (x_{22} \le \varepsilon_{22}) \tag{3}$$

Для x_{21} выбрана ε_{21} , (в рассматриваемом случае $\varepsilon_{21} = 0$). Если считать что $x_{11} = const = C_1$; $x_{22} = const = C_2$ на интервале $t \in [\, t_0, \hat{t}\,]$, то траектория движения системы S в пространстве состояний $\mathbb{X}$ будет иметь вид изображённый на рис. 2 кривой 1.

Допустим, что в момент $\tilde{t}$ изменилось значение переменной x_{11} с C_1 на C_3 и далее не менялось на $[\, \hat{t}, \tilde{t}\,]$, $C_1 < C_3$. Тогда, если на $[\, \hat{t}, \tilde{t}\,]$ x_{21} росла, то продолжение траектории S видно на рис. 2 (кривая 2).

Пусть в момент $\tilde{t}$ принято решение о "усечении" II рода блокчейна S. Тогда новым начальным состоянием блокчейна объявляется точка A_2. Сумма в кошельке есть $x_{21}(\tilde{t})$,

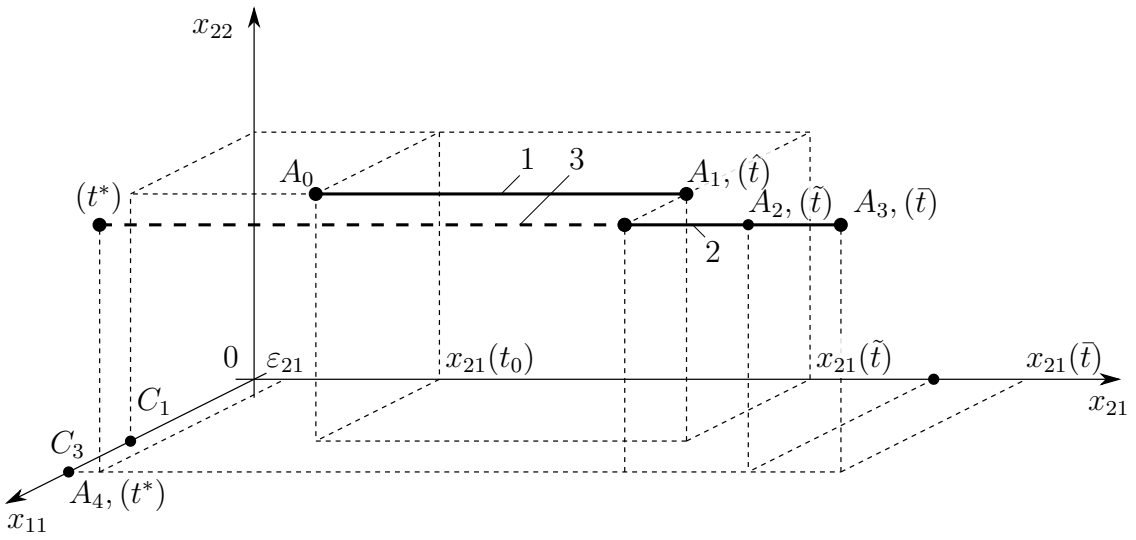

Рис. 2: Траектория системы из 2 блоков в трёхмерном пространстве состояний.

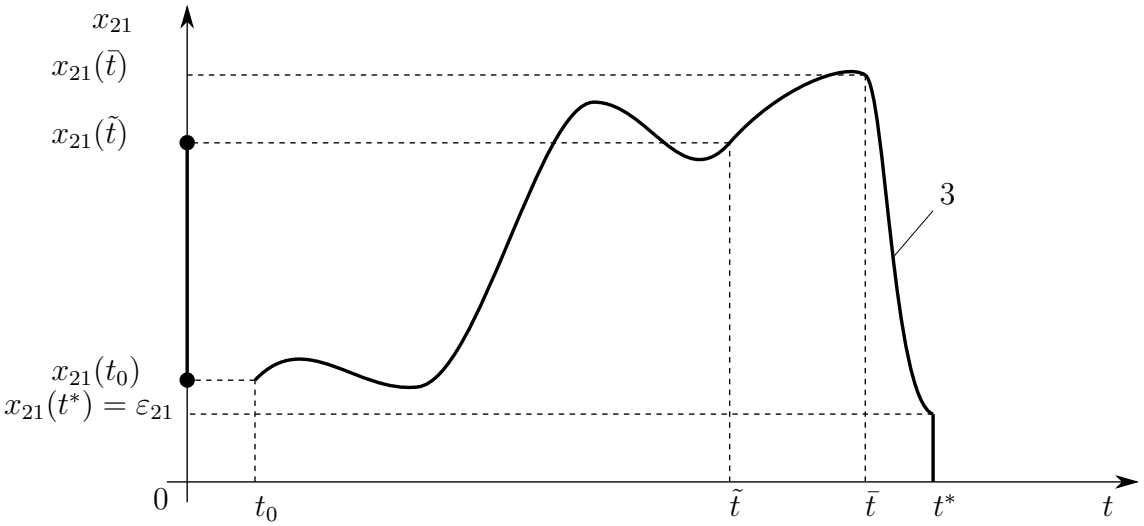

Рис. 3: График координаты x_{21} как функции времени.

способность открывать узлы сохраняется $x_{22} = 1$, G-блок "помнит" только адрес корневого узла C_3. Адрес "старого" корневого узла C_1 и он остаётся доступным в архиве. Движение продолжалось при $t \in [\tilde{t}, \bar{t}]$. Пусть на полуинтервале $[\bar{t}, t^*)$ переменные x_{11} и x_{22} не менялись, а x_{21} убывала до ε_{21} и при $t \geq t^*, x_{21} < \varepsilon_{21}$. В момент t^* x_{21} становится ε_{21}-нулевой и полагается равной нулю (кривая 3). Кошелёк теряет способность открывать узлы и ликвидируется, $x_{22} = 0$. Сумма $x_{21}(t^*)$ переводится, например, в системный кошелёк. Производится "усечение" блокчейна II рода, после которого рассматривается только $\mathbb{X}_1, \dim \mathbb{X}_1 = 1$ и до изменения x_{11} блокчейн с момента t^* находится в точке с координатами $(C_3, 0, 0) \in \mathbb{X}$.

5 Выводы

Представление блокчейна как динамической системы в пространстве состояний позволило рассмотреть вопрос усечения, согласовав свойства системных сущностей, наделённых существенно различными свойствами. Сохранение структуры пространства состояний после усечения его размерности позволяет утверждать, что предложенные подходы к усечению блокчейна дают корректный результат. Усечение блокчейна по времени и по фазовым

координатам позволяет существенно экономить ресурсы системы.

Список литературы

[1] Satoshi Nakamoto (2009). “Bitcoin: A Peer-to-Peer Electronic Cash System”. www.bitcoin.org .

[2] a@sumus.team, k@sumus.team, rr@sumus.team. “Consensus Algorithm for Bigger Blockchain Networks” (April 27, 2018).

[3] L.A.Zadeh, C.A.Desoer. Linear System Theory: The State Space Approach. Dover Publications, 2008, 656 p.