Блокчейн-платформа hschain и язык смартконтрактов

СЕРГЕЙ ЗЕФИРОВ, HEX Research, Россия
АЛЕКСЕЙ ХУДЯКОВ, HEX Research, Россия
АНТОН ХОЛОМЬЁВ, HEX Research, Россия

В статье представлен обзор платформы для реализации блокчейн-приложений hschain и языка смартконтрактов hschain-utxo. Платформа hschain позволяет создавать блокчейн приложения на языке Haskell в виде конечных автоматов, правила валидации транзакций являются переходами состояний и в отличие от многих решений не фиксированы, а являются интерфейсом. Этот гибкий подход даёт возможность построения различных систем основанных на технологии блокчейн.

CCS Concepts: • **proof of work**; • **Smartcontracts**; • **Blockchain**;

Additional Key Words and Phrases: blockchain, network, smartcontracts, proof of work

ACM Reference Format:
Сергей Зефиров, Алексей Худяков, and Антон Холомьёв. 2021. Блокчейн-платформа hschain и язык смартконтрактов. 1, 1 (April 2021), 8 pages. https://doi.org/10.1145/1122445.1122456

1 СРАВНЕНИЕ ПОДХОДОВ

Практически все современные системы доказательства работы основаны на переборе с отсевом: Bitcoin, Etherium, Monero, Ergo и многие другие следуют по стопам HashCash (перебираем значения нескольких составляющих блока и отсеиваем путём сравнения криптосуммы заголовка блока с некоторым значением), а PrimeCoin перебирает простые числа определённого вида.

В любом случае, это задача перебора.

Классическая задача перебора, с которой началась теория сложности, это решение задачи выполнимости для некоторой логической формулы. При каких значениях входов некоторая логическая формула является выполнимой? Зная решение, очень просто проверить его через подстановку значений и вычисления по структуре формулы. Однако отыскать решение решительно сложно.

2 ПОДРОБНЕЕ ПРО ЛОГИЧЕСКИЕ ЗАДАЧИ

Один из вариантов логической формулы является коньюнктивная нормальная форма (КНФ или CNF по английски) - логическое И логических ИЛИ, состоящих из одного или более литерала (литерал это либо значение переменной, либо инверсия значения переменной).

Обычно, КНФ строят из описания какой-либо логической схемы или задачи, однако один из вариантов построения КНФ это случайная КНФ с дизъюнктами (логическими ИЛИ) из заданного количества литералов, которые выбираются случайными образом. Такие случайные КНФ не несут какого-либо

Authors' addresses: Сергей Зефиров, HEX Research, Москва, Россия, larst@affiliation.org; Алексей Худяков, HEX Research, Королёв, Россия, larst@affiliation.org; Антон Холомьёв, HEX Research, Подольск, Россия.

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. Copyrights for components of this work owned by others than the author(s) must be honored. Abstracting with credit is permitted. To copy otherwise, or republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee. Request permissions from permissions@acm.org.
© 2021 Copyright held by the owner/author(s). Publication rights licensed to ACM.
XXXX-XXXX/2021/4-ART $15.00
https://doi.org/10.1145/1122445.1122456

смысла, тем не менее, они 1) так же сложны, как и КНФ для задач из практики, их решение отыскать так же сложно, 2) обычно, они имеют более, чем одно решение и 3) вероятность существования решения, сложность его отыскания и количество решений статистически определяются параметрами КНФ: количеством переменных, размером дизъюнкта и количеством дизъюнктов.

3 ЛОГИЧЕСКАЯ ЗАДАЧА, КАК ЧАСТЬ ФИЛЬТРА ДЛЯ ОТСЕВА БЛОКОВ

Что Bitcoin, что другие формируют заголовок блока и перебирают значения некоторых полей заголовка, чтобы получить криптосумму меньше, чем порог сложности. Обычно, это последнее поле заголовка - так называемый nonce (Number used Only oNCE), одноразовое число. Размер этого поля невелик, в районе 32-64 битов и никаких ограничений, кроме размера, на него не накладывается.

Мы предлагаем иметь большое одноразовое число, размером 256 битов, и наложить на него ограничение, что это поле содержит в себе решение для случайной КНФ с дизъюнктами из пяти литералов (от 256 переменных), состоящей из 5250 дизъюнктов. Случайная КНФ получается из криптосуммы части заголовка до одноразового числа. Криптосумма от полного заголовка блока (включая одноразовое число-решение) должна удовлетворять критерию сложности (быть меньше, чем порог сложности).

4 ПОИСК РЕШЕНИЯ, КАК ОГРАНИЧИВАЮЩИЙ ФАКТОР

Многие современные системы доказательства работы (PoW) предпочитают полагаться на пропускную способность канала с внешней памятью, нежели на простое вычисление относительно простой функции (SHA256d в случае Bitcoin). Это относится к Ergo, Monero, Etherium и многим другим. Считается, что пропускная способность памяти масштабируется тяжелее, чем простые вычисления (что справедливо).

Однако уверенного размена достичь довольно сложно. Например, если использовать scrypt, который сперва заполняет память с помощью последовательного применения криптосуммы, а потом производит произвольную выборку из памяти по случайным адресам, то легко разменять пропускную способность памяти на вычислительные мощности (писать в память только, допустим, каждое восьмое значение, а семь оставшихся вычислять - что, как показывает практика ASIC для Bitcoin, легко достижимо и очень и очень энергоэффективно). Что Etherium, что Ergo, что Monero/RandomX имеют сходную структуру и позволяют либо перевычислять значения, либо склеивать выборки из памяти, уменьшая эффективную задержку.

Использование пропускной способности памяти можно обобщить до алгоритма, заметная часть которого последовательна и связана с поддержанием какого-то сравнительно большого состояния.

Современные алгоритмы решения задач булевой выполнимости как раз таковы - заметная доля их выполнения последовательна. Для полных алгоритмов решения надо поддерживать дизъюнкты в разного рода списках и статистику для определения очередной переменной для расщепления выбора. Для алгоритмов решения методом случайного поиска необходимо использовать и поддерживать актуальную статистику по переменным и дизъюнктам после изменения решения хотя бы на один бит.

Параметры задачи (5250 дизъюнктов из пяти литералов от 256 переменных на данный момент) таковы, что отыскание хоть какого-то решения занимает полсекунды на современном процессоре. Поиск последующих решений несколько быстрее - порядка 3-4 миллисекунд, - однако иногда алгоритм снова может потратить несколько сотен микросекунд на поиск. Поэтому среднее количество решений в секунду составляет, примерно, 30-50 решений, или, поскольку время на вычисление полной криптосуммы загадки пренебрежимо мало, 30-50 криптозагадок в секунду. Это сравнимо с довольно медленным Monero/RandomX с его 200 ответов криптозагадок в секунду. Надо отметить, что здесь речь идёт не о полностью подходящих решениях (проходящих порог сложности), а всего лишь о каких-то кандидатах, некоторые из которых могут и подходить по сложности.

5 ПАРАЛЛЕЛЬНОЕ ВЫПОЛНЕНИЕ И ASIC

Как ни странно, но на GPU современные методы решения задач булевой выполнимости укладываются довольно посредственно. Это связано с необходимостью поддержания своей копии статистики для каждого (частичного) решения, а эта статистика занимает довольно большой объём и находится в существенно далёких областях памяти. Поэтому: с одной стороны, всего 256 битов/переменных, с другой стороны 5250 ограничений, по разному связанных с этими битами. В сумме получается 128К на хранение статистики для решения и выше. Настолько большое расстояние, плюс одновременное выполнение команд на всех ядрах блока нитей GPU приводит к слабой утилизации вычислительных возможностей GPU.

Однако, 128 килобайт не так, чтобы и много для памяти около специализированного ядра в ASIC. Это, примерно, 12 квадратных миллиметров, по моим прикидкам. То есть, возможно получить довольно производительную систему с помощью программирования на Verilog/VHDL, если нам такое понадобится.

6 ОСНОВНЫЕ СВОЙСТВА

При уменьшении порога вдвое время на поиск решения увеличивается, примерно, вдвое. Таким образом мы можем прогнозировать, как скажется изменение порога сложности на производительности PoW.

Фиксация части переменных для разбиения на подзадачи работает довольно плохо. Если мы знаем решение задачи и подаём на решатель задачц, в которой части этого решения уже зафиксирована (например, если есть решение с x0=Ложь, то мы создаём обычную задачу и добавляем дизхюнкт из одного литерала !x0), то решатель совершенно необязательно сможет отыскать решение, вроде бы, более простой задачи. Поэтому поиск решения лучше выполнять последовательно, для одного заголовка.

Поиск разных решений осуществляется добавлением ограничения, отсекающего текущее решение. Это, во-первых, увеличивает количество ограничений и время на их обработку и, во-вторых, всё более меняет структуру задачи. Если раньше она была случайной задачей из 5-литеральных дизъюнктов, то теперь среднее количество литералов увеличивается и эвристики перестают работать - увеличивая время поиска решения ещё больше.

7 ЗАКЛЮЧЕНИЕ

Мы предлагаем использовать решение случайной задачи булевой выполнимости, в качестве основной загадки для системы доказательства работы.

Это, с одной стороны, очень простая в формулировке задача, с другой стороны, её исследуют вот уже 50 лет с умеренным успехом и современное состояние дел не позволяет решать её очень быстро. А прогресс за последние десятилетия позволяет прогнозировать, что и в ближайшем будущем решение такого рода задач не будет ускорено сколько-нибудь сильно.

В настоящий момент у нас есть работающий код для предлагаемого варианта PoW. У нас, также, есть опыт создания решений для FPGA для похожих задач, поэтому мы сможем предложить сотрудничество для желающих создавать ASIC решения для нашей системы PoW.

8 SECTIONING COMMANDS

Your work should use standard LaTeX sectioning commands: section, subsection, subsubsection, and paragraph. They should be numbered; do not remove the numbering from the commands.

Simulating a sectioning command by setting the first word or words of a paragraph in boldface or italicized text is **not allowed.**

Таблица 1. Frequency of Special Characters

Non-English or Math	Frequency	Comments
Ø	1 in 1,000	For Swedish names
π	1 in 5	Common in math
\$	4 in 5	Used in business
Ψ_1^2	1 in 40,000	Unexplained usage

Таблица 2. Some Typical Commands

Command	A Number	Comments
\author	100	Author
\table	300	For tables
\table*	400	For wider tables

9 TABLES

The "acmart" document class includes the "booktabs" package — https://ctan.org/pkg/booktabs — for preparing high-quality tables.

Table captions are placed *above* the table.

Because tables cannot be split across pages, the best placement for them is typically the top of the page nearest their initial cite. To ensure this proper "floating" placement of tables, use the environment **table** to enclose the table's contents and the table caption. The contents of the table itself must go in the **tabular** environment, to be aligned properly in rows and columns, with the desired horizontal and vertical rules. Again, detailed instructions on **tabular** material are found in the *LaTeX User's Guide*.

Immediately following this sentence is the point at which Table 1 is included in the input file; compare the placement of the table here with the table in the printed output of this document.

To set a wider table, which takes up the whole width of the page's live area, use the environment **table*** to enclose the table's contents and the table caption. As with a single-column table, this wide table will "float" to a location deemed more desirable. Immediately following this sentence is the point at which Table 2 is included in the input file; again, it is instructive to compare the placement of the table here with the table in the printed output of this document.

10 MATH EQUATIONS

You may want to display math equations in three distinct styles: inline, numbered or non-numbered display. Each of the three are discussed in the next sections.

10.1 Inline (In-text) Equations

A formula that appears in the running text is called an inline or in-text formula. It is produced by the **math** environment, which can be invoked with the usual \begin ...\end construction or with the short form $ ...$. You can use any of the symbols and structures, from α to ω, available in LaTeX [**?**]; this section will simply show a few examples of in-text equations in context. Notice how this equation: $\lim_{n\to\infty} x = 0$, set here in in-line math style, looks slightly different when set in display style. (See next section).

10.2 Display Equations

A numbered display equation—one set off by vertical space from the text and centered horizontally—is produced by the **equation** environment. An unnumbered display equation is produced by the **displaymath** environment.

Again, in either environment, you can use any of the symbols and structures available in LaTeX; this section will just give a couple of examples of display equations in context. First, consider the equation, shown as an inline equation above:

$$\lim_{n \to \infty} x = 0 \tag{1}$$

Notice how it is formatted somewhat differently in the **displaymath** environment. Now, we'll enter an unnumbered equation:

$$\sum_{i=0}^{\infty} x + 1$$

and follow it with another numbered equation:

$$\sum_{i=0}^{\infty} x_i = \int_{0}^{\pi+2} f \tag{2}$$

just to demonstrate LaTeX's able handling of numbering.

11 FIGURES

The "figure" environment should be used for figures. One or more images can be placed within a figure. If your figure contains third-party material, you must clearly identify it as such, as shown in the example below.

Your figures should contain a caption which describes the figure to the reader. Figure captions go below the figure. Your figures should **also** include a description suitable for screen readers, to assist the visually-challenged to better understand your work.

Figure captions are placed *below* the figure.

11.1 The "Teaser Figure"

A "teaser figure" is an image, or set of images in one figure, that are placed after all author and affiliation information, and before the body of the article, spanning the page. If you wish to have such a figure in your article, place the command immediately before the \maketitle command:

```
\begin{teaserfigure}
  \includegraphics[width=\textwidth]{sampleteaser}
  \caption{figure caption}
  \Description{figure description}
\end{teaserfigure}
```

12 CITATIONS AND BIBLIOGRAPHIES

The use of BibTeX for the preparation and formatting of one's references is strongly recommended. Authors' names should be complete — use full first names ("Donald E. Knuth") not initials ("D. E. Knuth") — and the salient identifying features of a reference should be included: title, year, volume, number, pages, article DOI, etc.

The bibliography is included in your source document with these two commands, placed just before the \end{document} command:

```
\bibliographystyle{ACM-Reference-Format}
\bibliography{bibfile}
```

Fig. 1. 1907 Franklin Model D roadster. Photograph by Harris & Ewing, Inc. [Public domain], via Wikimedia Commons. (https://goo.gl/VLCRBB).

where "bibfile" is the name, without the ".bib" suffix, of the BibTeX file.

Citations and references are numbered by default. A small number of ACM publications have citations and references formatted in the "author year" style; for these exceptions, please include this command in the **preamble** (before "\begin{document}") of your LaTeX source:

\citestyle{acmauthoryear}

Some examples. A paginated journal article [**?**], an enumerated journal article [**?**], a reference to an entire issue [**?**], a monograph (whole book) [**?**], a monograph/whole book in a series (see 2a in spec. document) [**?**], a divisible-book such as an anthology or compilation [**?**] followed by the same example, however we only output the series if the volume number is given [**?**] (so Editor00a's series should NOT be present since it has no vol. no.), a chapter in a divisible book [**?**], a chapter in a divisible book in a series [**?**], a multi-volume work as book [**?**], an article in a proceedings (of a conference, symposium, workshop for example) (paginated proceedings article)

[**?**], a proceedings article with all possible elements [**?**], an example of an enumerated proceedings article [**?**], an informally published work [**?**], a doctoral dissertation [**?**], a master's thesis: [**?**], an online document / world wide web resource [**? ? ?**], a video game (Case 1) [**?**] and (Case 2) [**?**] and [**?**] and (Case 3) a patent [**?**], work accepted for publication [**?**], 'YYYYb'-test for prolific author [**?**] and [**?**]. Other cites might contain 'duplicate' DOI and URLs (some SIAM articles) [**?**]. Boris / Barbara Beeton: multi-volume works as books [**?**] and [**?**]. A couple of citations with DOIs: [**? ?**]. Online citations: [**? ? ?**].

13 ACKNOWLEDGMENTS

Identification of funding sources and other support, and thanks to individuals and groups that assisted in the research and the preparation of the work should be included in an acknowledgment section, which is placed just before the reference section in your document.

This section has a special environment:

```
\begin{acks}
...
\end{acks}
```

so that the information contained therein can be more easily collected during the article metadata extraction phase, and to ensure consistency in the spelling of the section heading.

Authors should not prepare this section as a numbered or unnumbered \section; please use the "acks" environment.

14 APPENDICES

If your work needs an appendix, add it before the "\end{document}" command at the conclusion of your source document.

Start the appendix with the "appendix" command:

```
\appendix
```

and note that in the appendix, sections are lettered, not numbered. This document has two appendices, demonstrating the section and subsection identification method.

15 SIGCHI EXTENDED ABSTRACTS

The "sigchi-a" template style (available only in LaTeX and not in Word) produces a landscape-orientation formatted article, with a wide left margin. Three environments are available for use with the "sigchi-a" template style, and produce formatted output in the margin:

- sidebar: Place formatted text in the margin.
- marginfigure: Place a figure in the margin.
- margintable: Place a table in the margin.

ACKNOWLEDGMENTS

To Robert, for the bagels and explaining CMYK and color spaces.

A RESEARCH METHODS

A.1 Part One

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Morbi malesuada, quam in pulvinar varius, metus nunc fermentum urna, id sollicitudin purus odio sit amet enim. Aliquam ullamcorper eu ipsum vel mollis. Curabitur quis dictum nisl. Phasellus vel semper risus, et lacinia dolor. Integer ultricies commodo sem nec semper.

A.2 Part Two

Etiam commodo feugiat nisl pulvinar pellentesque. Etiam auctor sodales ligula, non varius nibh pulvinar semper. Suspendisse nec lectus non ipsum convallis congue hendrerit vitae sapien. Donec at laoreet eros. Vivamus non purus placerat, scelerisque diam eu, cursus ante. Etiam aliquam tortor auctor efficitur mattis.

B ONLINE RESOURCES

Nam id fermentum dui. Suspendisse sagittis tortor a nulla mollis, in pulvinar ex pretium. Sed interdum orci quis metus euismod, et sagittis enim maximus. Vestibulum gravida massa ut felis suscipit congue. Quisque mattis elit a risus ultrices commodo venenatis eget dui. Etiam sagittis eleifend elementum.

Nam interdum magna at lectus dignissim, ac dignissim lorem rhoncus. Maecenas eu arcu ac neque placerat aliquam. Nunc pulvinar massa et mattis lacinia.