УДК: 004.03, 004.72

Об эффективных механизмах обеспечения надежности цифровых платформ

D.F. Aliev, A.Yu. Shcherbakov

On Effective Mechanisms for Ensuring the Reliability of Digital Platforms

Abstract. *This article is devoted to the formulation of the architectural conditions for acceptance and the correct economic model of the platform. An approach is proposed that combines the mechanisms Proof of History and Proof of Useful Work, which make it possible to create on the platform, including scientometric and qualimetric, data chains, where integrity and evidence-based consistency is protected by cryptographic methods, and the functionality and reliability of the platform are provided through the processes of indexing and comparing texts (the core of the semantic service). The concepts of non-inflationary and controlled-inflationary platform are considered.*

Keywords: *acceptance, trust, non-inflationary platform, controlled-inflationary platform, scientometric platform, qualimetric platform, proof of useful work (PoUW), proof of history (PoH), cryptographic method.*

Д.Ф.Алиев[1]
А.Ю.Щербаков[2]
[1]Доктор философии в области бизнес-права (PhD), доктор делового администрирования в области финансов (DBA), кандидат экономических наук, первый проректор Федерального государственного бюджетного образовательного учреждения высшего образования «Российский государственный социальный университет».
E-mail: kharchenkoDD@rgsu.net
[2]Доктор технических наук, заведующий кафедрой когнитивно-аналитических и нейро-прикладных технологий РГСУ, ведущий научный сотрудник Государственного университета управления.
E-mail: x509@ras.ru

Аннотация. *Статья посвящена формулированию архитектурных условий акцептности и корректной экономической модели платформы. Предлагается подход, объединяющий механизмы доказательства истории (Proof-of-History) и доказательства полезной работы (Proof-of-Useful-Work), в рамках которого возможно создание на платформе, в том числе наукометрической и квалиметрической, цепочек данных, целостность и доказательная последовательность которых защищена криптографическими методами, а функциональность и надежность платформы обеспечиваются за счет процессов индексирования и сравнения текстов (ядро семантического сервиса). Рассматриваются понятия безынфляционной и управляемо-инфляционной платформы.*

Ключевые слова: *акцептность, доверие, безынфляционная платформа, управляемо-инфляционная платформа, наукометрическая платформа, квалиметрическая платформа, доказательство полезной работы, доказательство истории, криптографический метод.*

ВВЕДЕНИЕ

В настоящее время весьма важными в теоретической и практической информатике являются несколько вопросов, связанных с развитием цифровых платформ будущего, в том числе и платформ искусственного интеллекта. Эти проблемы касаются в первую очередь акцептности (адекватности и добровольности принятия пользователями) тех услуг и сервисов, которые предоставляет платформа, корректной экономической модели платформы, поддерживающей оборот как цифровых финансовых активов (ЦФА), так и реальных фиатных средств, а также соблюдения законодательств и прав пользователей платформы.

Все эти проблемы могут быть решены как организационно-методическими и законодательными мерами, так и продуманными решениями в архитектуре платформы.

ПОСТАНОВКА ЗАДАЧИ

Вполне очевидно, исходя из прецедентного развития техники и экономики, что цифровые платформы будут ориентироваться на эффективный учет трудозатрат на получение разного рода услуг пользователями и участниками платформы.

Здесь важно заметить, что кроме пользователей и операторов в платформах возникает участник, который косвенно пользуется услугами платформы и вполне может является прямым или косвенным выгодоприобретателем платформенных услуг.

Например, участниками платформы почтового или новостного портала являются рекламодатели,

а платформы подбора работников – работодатели. Пользователи могут быть и участниками платформы (например, формирование видеороликов может приносить доход).

При проектировании и реализации платформы технически целесообразно, а в некоторых случаях - необходимо учитывать и реализовывать механизмы распределенных систем (например, распределенных реестров), а для операционных или транзакционных платформ использовать разного рода механизмы консенсуса участников и пользователей, либо механизмы создания связанных цепочек различных событий или данных платформы.

Например, для наукометрических и квалиметрических платформ необходима реализация механизма «доказательства истории» (Proof-of-History, PoH), который заключается в том, что события на платформе (в частности, поступление научных материалов для депонирования или рецензирования) происходят в доказательной последовательности, когда один материал доказательно поступил на платформу раньше другого.

Для реализации PoH необходимо создание цепочек данных, целостность и последовательность которых защищена криптографическими методами (код аутентификации), службы оператора платформы, добавляющего в цепочки данных метки реального времени, на которые ориентируются пользователи и участники платформы, а также осуществление выдачи квитанций пользователям и участникам о совершении ими действий и параметрах протокола PoH.

Авторами статьи предлагается подход, объединяющий механизмы PoH и доказательства работы (Proof-of-Work, PoW). При этом доказательство работы может быть реализовано в виде копирования изменений данных платформы на другие ее распределенные элементы (ноды), либо на удаленный ресурс, который доступен для записи, но недоступен для изменений даже оператору платформы («Writy-only»).

Преимуществами данного подхода, в первую очередь, являются снижение непроизводительных затрат на реализацию доказательства работы и защита целостности и отказоустойчивости данных в рамках платформы.

В принципе механизм PoW такого рода становится уже доказательством полезной работы (Proof-of-Useful-Work, PoUW) поскольку не использует необязательных операций, связанных с затратой ресурсов платформы (в биткойне PoW связан со значительным расходом электрической энергии для генерации хеш-значений определенного вида), а обеспечивает функциональность и надежность платформы.

Механизм резервного переноса информации может быть дополнен и другими механизмами доказательства полезной работы. Полезная работа в наукометрических платформах может быть связана также с индексированием информации [1]. В этом случае платформа приобретает весьма доказательную экономику.

ПОНЯТИЯ БЕЗЫНФЛЯЦИОННОЙ И УПРАВЛЯЕМО-ИНФЛЯЦИОННОЙ ПЛАТФОРМЫ

Рассмотрим финансово гетерогенную платформу, в которой обращаются токены. Токены можно обменять в любое удобное пользователям и участникам системы время на фиатные средства. Обмен производится с реализаций локальных процедур (например, для трансграничной платформы – в рамках национального законодательства о банковской деятельности и платежных системах), с участием финансовой (ФО) или кредитной организации (КО) в рамках отношений гражданско-правового характера, когда в обмен на некоторое количество токенов пользователь (участник) получает стандартные платежные инструменты от ФО или КО в соответствии с курсом обмена токенов на фиатные средства.

Назовем платформу безынфляционной, если совокупность ассоциированных с ней фиатных средств обеспечена детерминированной публичной процедурой обмена токенов на данные фиатные средства с полным их покрытием.

Назовем платформу управляемо-инфляционной, если в ней реализованы механизмы фьючерсного поведения или векселя, позволяющие владельцам токенов получать фиатные средства в будущем.

В качестве примера рассмотрим квалиметрическую платформу Сешат [2].

1. Регистрация пользователей на платформе

Пользователь вводит свое имя, получает анонимное имя UserX [3], вырабатывает свой ключ в ключевом контейнере, защищенном паролем. Загружает свои квалификационные документы (диплом об образовании, ученом звании и степени, список трудов, другую необходимую информацию). Далее пользователь заполняет анкету, где указывает тематики, по которым он дает рецензии или проводит экспертизы (если он претендует на роль эксперта).

Администратор верификации производит верификацию загруженных документов и самого поль-

зователя и завершает его регистрацию. Пользователь получает статус – одну или несколько ролей и перечень тематик, в которых он компетентен. Параметры пользователя отражены в его профиле.

2. Загрузка статей (документов)

Статьи загружаются для рецензирования или депонирования. Во втором случае рецензирование не требуется, фиксируется приоритет; депонированию также подвергаются статьи или работы с требованиями сохранения конфиденциальности.

При загрузке производится индексирование статьи и установление ее принадлежности к тематике.

Индексирование статей может производить пользователь или участник платформы перед их загрузкой или в процессе загрузки и получать за это цифровые финансовые активы (токены).

После успешной загрузки статьи администратор рецензий направляет ее на рецензирование или депонирование.

При загрузке и поиске используется ядро семантического сервиса (процессы индексирования и сравнения текстов), которое реализует в системе PoUW.

Весьма важным для акцептности платформы является получение пользователем подписанных квитанций, которые с одной стороны, дают доказательство, что пользователь загрузил, а система приняла документы, а с другой – фиксируют объем полезной работы, выполненный пользователем или участником платформы.

Пример квитанции платформы «Сешат»

DNum : 55
TNum :9c16dc924ea4c1174de1357f2e1ac594
Sign :cc0cb88a087d495c
File :c2.txt
NetName:429398babb45cb580000000000000000
Token: 8
AddTime:11:34:09 14.02.0023

3. Рецензирование статей

Рецензент по публичной методике выставляет оценки статье и обосновывает их в виде рецензии, которую подписывает своей электронной подписью (ЭП).

Рецензии и оценки модерируются администратором рецензий (например, в целях дополнительной анонимизации эксперта для исключения выяснения его личности и исключения давления на него).

Возможен режим без модерации, когда собираются оценки и рецензии не менее трех экспертов и автору направляется только усредненное мнение (оценка).

4. Начисление токенов за рецензии и статистика

После формирования рецензии и оценки экспертам начисляются токены в соответствии с их рейтингом.

Возможна ситуация, когда реальных токенов (начисленных авторами, спонсорами или внешними заказчиками) не хватает для оплаты работы экспертов, в этом случае начисленные токены маркируются как кредитные (вексель) и учитываются по мере появления реальных токенов в хронологической очередности оплаты услуг экспертов. В случае допустимости режима управляемой инфляционности возможен обмен и необеспеченных токенов, либо гибкое изменение курса их обмена.

Все действия регистрируются в журналах с соблюдением PoH.

5. Работа внешних заказчиков (участников платформы)

Внешний заказчик регистрируется отдельно и также проходит процедуру верификации как физическое или юридическое лицо. Он также является донором (поставщиком) токенов (цифровых финансовых активов, ЦФА), при этом токены обеспечены реальными деньгами, которые участник вносит на ассоциированный с платформой расчетный счет (счетов может быть несколько).

Он имеет возможность знакомиться со статистикой поступления статей, оценками за них, а также отдельно оплачивать процедуры развернутого поиска – когда его текстовый запрос сравнивается со статьями тематики с учетом заданного порога их рейтинга (средней экспертной оценки). Поиск может происходить и только по рейтингу статей.

К внешним заказчикам также относятся эксперты государственных учреждений и сервисов, которые обращаются за фактами приоритета или плагиата, различными характеристиками научных достижений авторов или экспертов.

Приведем пример функции добавления записи в реестр с соблюдением PoH.

```
int OutFile(char *outname, unsigned char *dnum, unsigned char *ntran, unsigned char *buf, int buflen, unsigned char *imi,unsigned char *tdt)
  {
   FILE *fl;
   int l1,l2,l3,l4,l5,l6,l7,i;
   unsigned char dnum1[16];
   for(i=0;i<16;i++) dnum1[i]=dnum[i];
   for(i=0;i<8 ;i++) dnum1[i]= imi[i];

   if(if_exist(outname)==-1)  fl=fopen(outname,"wb");
   else                       {fl=fopen(outname,"r+b");fseek(fl,
```

```
0,SEEK_END);}
    if(fl!=NULL)
     {
Запись в структуру реестра
      Номер записи по порядку
      l1=fwrite(dnum   ,1,    16,fl);
     хеш или случайный номер (идентификатор транзакции)
      l2=fwrite(ntran  ,1,    16,fl);
      время-дата
      l3=fwrite(tdt    ,1,     8,fl);
      содержание записи
      l4=fwrite(buf    ,1,buflen,fl);
      хеш цепочки, включающий хеш предыдущей записи и всех информационных полей
      l6=fwrite(imi    ,1,     8,fl);
      длина записи
      l5=fwrite(&buflen,4,     1,fl);
      номер записи , увеличенный на единицу (для синхронизации со следующей записью)
      l7=fwrite(dnum1  ,1,    16,fl);
      fclose(fl);
     }
    else return(-1);
Проверка правильности записи
   if((l1+l2+l3+l4+l5+l6+l7)!=(buflen+81-16)) return(-2);
    return(0);
   }
Чтение реестра для создания цепочки РоН
int ReadRFile(char *outname,unsigned char *dnum, unsigned char *ntran,unsigned char *tdt, unsigned char *buf, unsigned char *imi)
   {
    FILE *fl;
    int l1,l2,l3,l4,l5,l6,l7,i;
    unsigned long buflen;
    unsigned char dnum1[16],ntrans1[16];

    if(if_exist(outname)==0) fl=fopen(outname,"rb");
    else return(-1);

    if(fl!=NULL)
     {
      fseek(fl,-20,SEEK_END);
      l1=fread(&buflen,4,     1,fl);
      fseek(fl,-(buflen+68),SEEK_END);

      l2=fread(dnum   ,1,    16,fl);
      l3=fread(ntran  ,1,    16,fl);
      l4=fread(tdt    ,1,     8,fl);
      l5=fread(buf    ,1,buflen,fl);
      l6=fread(imi    ,1,     8,fl);
      l7=fread(dnum1  ,1,    16,fl);
       fclose(fl);
      }
    else return(-1);
   if((l1+l2+l3+l4+l5+l6+l7)!=(buflen+81-16)) return(-2);
//      printf("%d %d %d\n",l1+l2+l3+l4+l5+l6+l7,l5,buflen+81-16);

    return(buflen);
   }
```

Следующая процедура формирует квитанцию при успешной записи в реестр:
fname – имя файла квитанции;
dnum1 – децимальный номер квитанции, соответствует номеру рестровой записи;
ntrans – хеш записи;
imi – имитовставка – хеш цепочки записей;
netname – сетевое имя пользователя платформы;
fname1 – имя записанного в реестр файла;
tdt – параметры времени и даты.

```
int MkKvit(char *fname,unsigned char *dnum1,unsigned char *ntrans, unsigned char *imi,unsigned char *netname, unsigned char *fname1,unsigned char *tdt)
   {
    FILE *out;
    int i,dnum3;
    out=fopen(fname,"wb");
    if(out==NULL) return(-1);

    dnum3=uint8ToUint32(dnum1+12);

    fprintf(out,"DNum   :");
    fprintf(out,"%d\n",dnum3);
    fprintf(out,"TNum   :");
    for(i=0;i<16;i++) fprintf(out,"%02x",ntrans[i]);
    fprintf(out,"\n");
    fprintf(out,"Sign   :");
    for(i=0;i< 8;i++) fprintf(out,"%02x",imi[i]);
    fprintf(out,"\n");
    fprintf(out,"File   :%s\n",fname1);
    fprintf(out,"NetName:");
    for(i=0;i<32;i++) fprintf(out,"%c",netname[i]);
    fprintf(out,"\n");
    fprintf(out,"AddTime:%02d:%02d:%02d%02d.%02d.%04d\n",
    tdt[0],tdt[1],tdt[2],tdt[3],tdt[4],tdt[5]);
   }
```

ГИПОТЕЗА О КОРРЕКТНОЙ ПЛАТФОРМЕ

Для реализации безынфляционной модели плат-

формы в нее должен быть встроен алгоритм доказательства полезной работы как для участников, так и для пользователей платформы.

Консенсус доказательства работы, применяемый в криптовалютах начального поколения (которые обладают высокой волатильностью), не ориентирован на безынфляционные модели.

В рассмотренной нами платформе и некоторых других системах в качестве PoUW используется алгоритм индексации текстов.

Важным для соблюдения прав пользователей является формирование квитанций о выполнении услуги на платформе. Кроме того, обязательна реализация криптографических механизмов для аутентификации пользователей и защиты передаваемой между ними и платформой информации.

Параметром полезной работы может быть количество проиндексированных единиц информации или скорость такой индексации.

Рассмотрим работу модуля индексации для статьи длиной 285 633 байта, файл c2.txt.

M_ind procedure- indexed text file. Project A
File length: 285633 Index page size: 278
File: c2.txt
Read: 16384 bytes. Part 1 of 18 [05%]
Words: 1
Medium word length: 1.000000
Word in LMD: 1
Words: 201
Medium word length: 5.363184
Word in LMD: 123
Words: 401
…
Medium word length: 5.244253
Word in LMD: 5506
Words: 42001
Medium word length: 5.247042
Word in LMD: 5507
Words: 42201
Medium word length: 5.250160
Word in LMD: 5508
Words: 42401
Medium word length: 5.250018
Word in LMD: 5537
Words: 42601
Medium word length: 5.243985
Word in LMD: 5548
Time: 34.409000 sec
Total words: 42757
Words per sec: 1242
Original length = 285633 Compress = 128271[44]
Sum=5548 [5548]
Spektr for dictionary
0->0.000000
1->0.006489
2->0.032084
3->0.060382
4->0.109769
5->0.126352
6->0.121485
7->0.143836
8->0.116979
9->0.094088
10->0.075523
11->0.045422
12->0.029740
13->0.018565
14->0.007751
15->0.005227
Sum=[0.993691] Medium len for DIC = 6.881039
Spektr for text
0->0.000000
1->0.051711
2->0.146666
3->0.172252
4->0.131417
5->0.101130
6->0.076198
7->0.086582
8->0.070211
9->0.052857
10->0.048881
11->0.027551
12->0.015179
13->0.012489
14->0.003368
15->0.001357
Sum=[0.993691]
Words = 42664 [42757]

Таким образом, пользователем платформы при загрузке статьи была выполнена полезная работа по индексации, которая заняла 34.4 секунды, за это время было проиндексировано 42757 слов со средней скоростью 1242 слова в секунду. За полезную работу пользователю начислено 8 токенов, что подтверждено заверенной (подписанной ЭП) квитанцией.

Применение подхода PoUW в рамках платформ можно также распространить на частичное обучение нейросетей.

ВЫВОДЫ

Для обеспечения свойств акцептности и безынфляционности платформы в ней целесообразно

реализовать доказательство полезной работы, связанное с начислением токенов. Курс обмена токенов должен быть установлен исходя из возможного полного покрытия ассоциированных с платформой фиатных средств.

Важным для соблюдения прав пользователей и участников является формирование на платформе квитанций о совершении ими действий и выполнении услуг.

Кроме того, обязательна реализация криптографических механизмов для аутентификации пользователей и защиты информации, передаваемой между ними и платформой.

Параметром полезной работы может быть количество проиндексированных единиц информации или скорость такой индексации, либо количество объектов, использованных для обучения (для семантических систем обучающими наборами являются тексты).

СПИСОК ЛИТЕРАТУРЫ

1. Щербаков А.Ю. О новом методе обеспечения безопасности семантических вычислений // Вестник современных цифровых технологий. 2022. № 12. С. 7-10.

2. Алиев Д.Ф., Щербаков А.Ю., Бородулина С.А. Актуальные подходы к квалиметрии и наукометрии // Вестник современных цифровых технологий. 2022. № 12. С. 11-20.

3. Алиев Д.Ф., Щербаков А.Ю. О практических подходах к созданию доверенных защищенных цифровых платформ // Вестник современных цифровых технологий. 2022. № 13. С. 4-12.