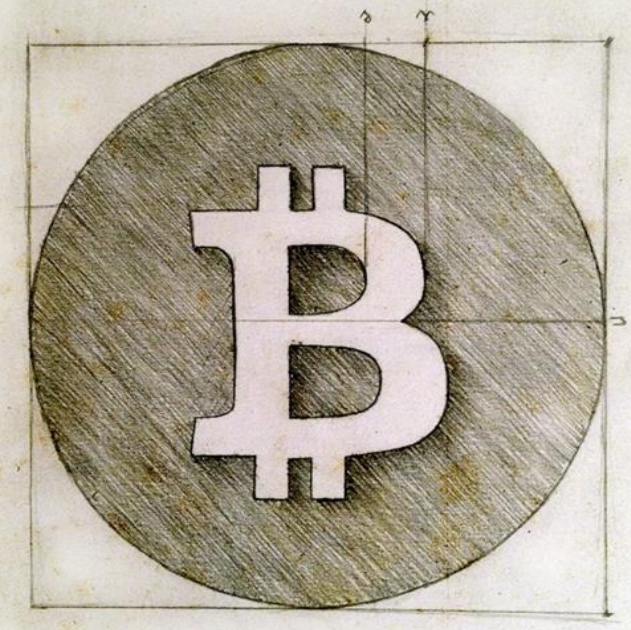


БЕЗОПАСНОСТЬ ТЕХНОЛОГИИ BLOCKCHAIN. ОСНОВНЫЕ НАПРАВЛЕНИЯ ИССЛЕДОВАНИЙ И АНАЛИЗ НАУЧНЫХ ПУБЛИКАЦИЙ

Директор по развитию ЗАО «БЕЛТИМ СБ»

директор ассоциации «РусКрипто», КОМИСАРЕНКО В.В.

Специалист по информационной безопасности

РОГОВОЙ А.С.

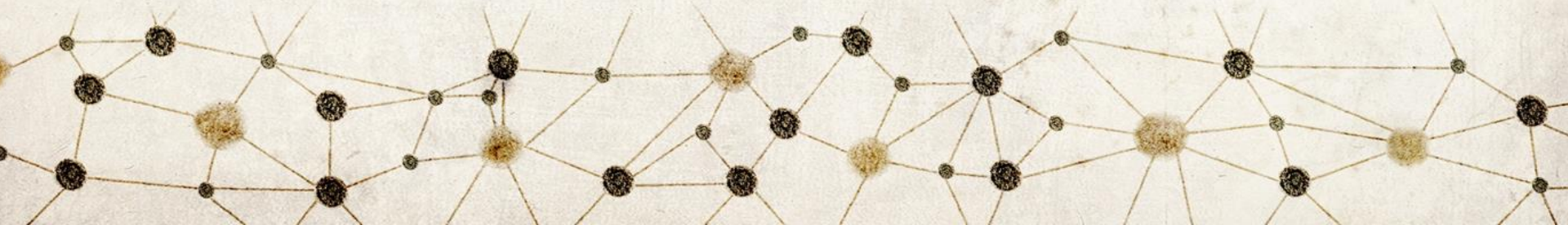
Почему нам интересна проблематика криптовалют и блокчейч?

1 Это реальность

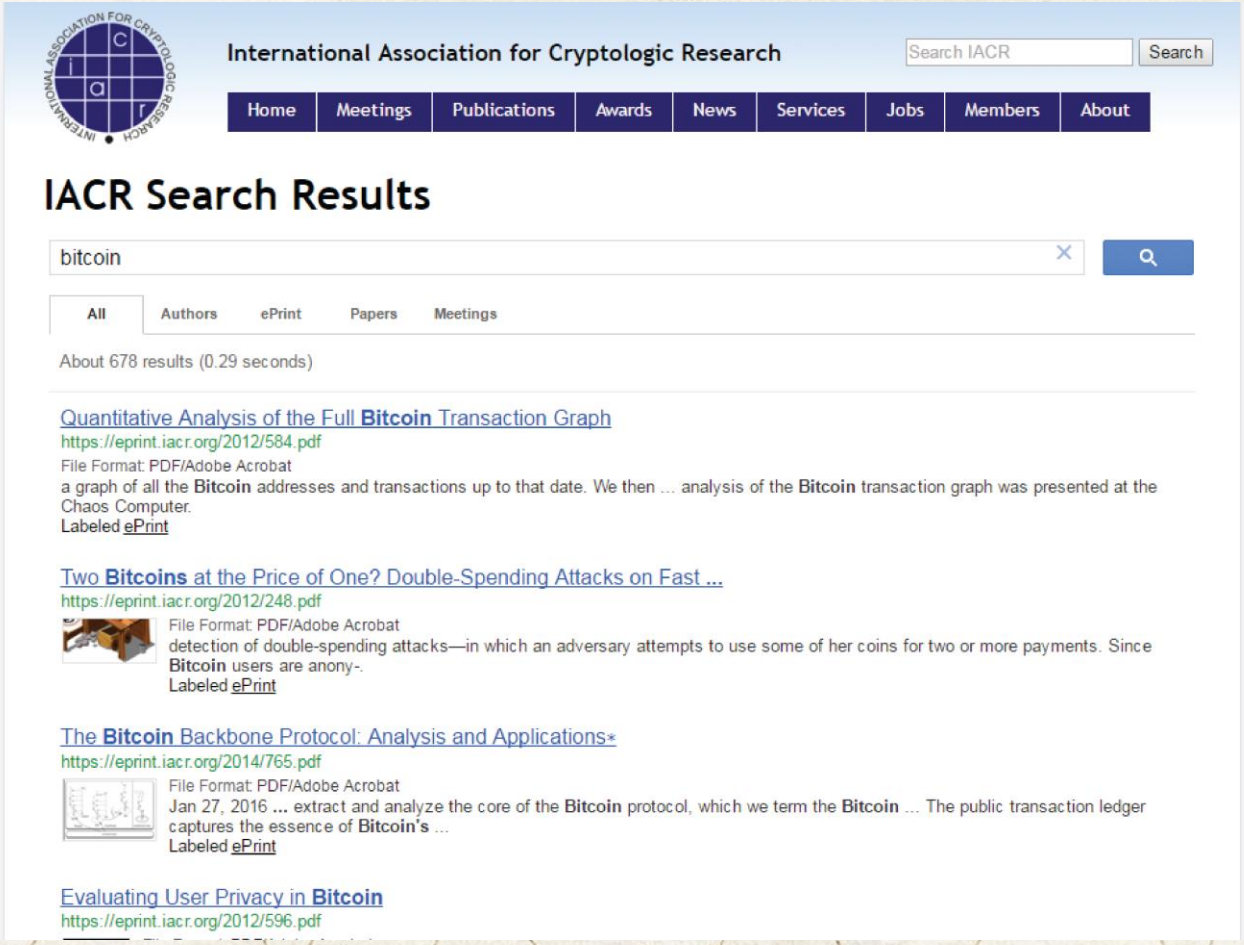
2 Это криптотехнологии

3 Это инновация, требующая оценки

4 Эта проблематика рассматривается на криптографических конференциях



Исследования Биткоина



International Association for Cryptologic Research

Search IACR | Search

Home | Meetings | Publications | Awards | News | Services | Jobs | Members | About

IACR Search Results

bitcoin

All | Authors | ePrint | Papers | Meetings

About 678 results (0.29 seconds)

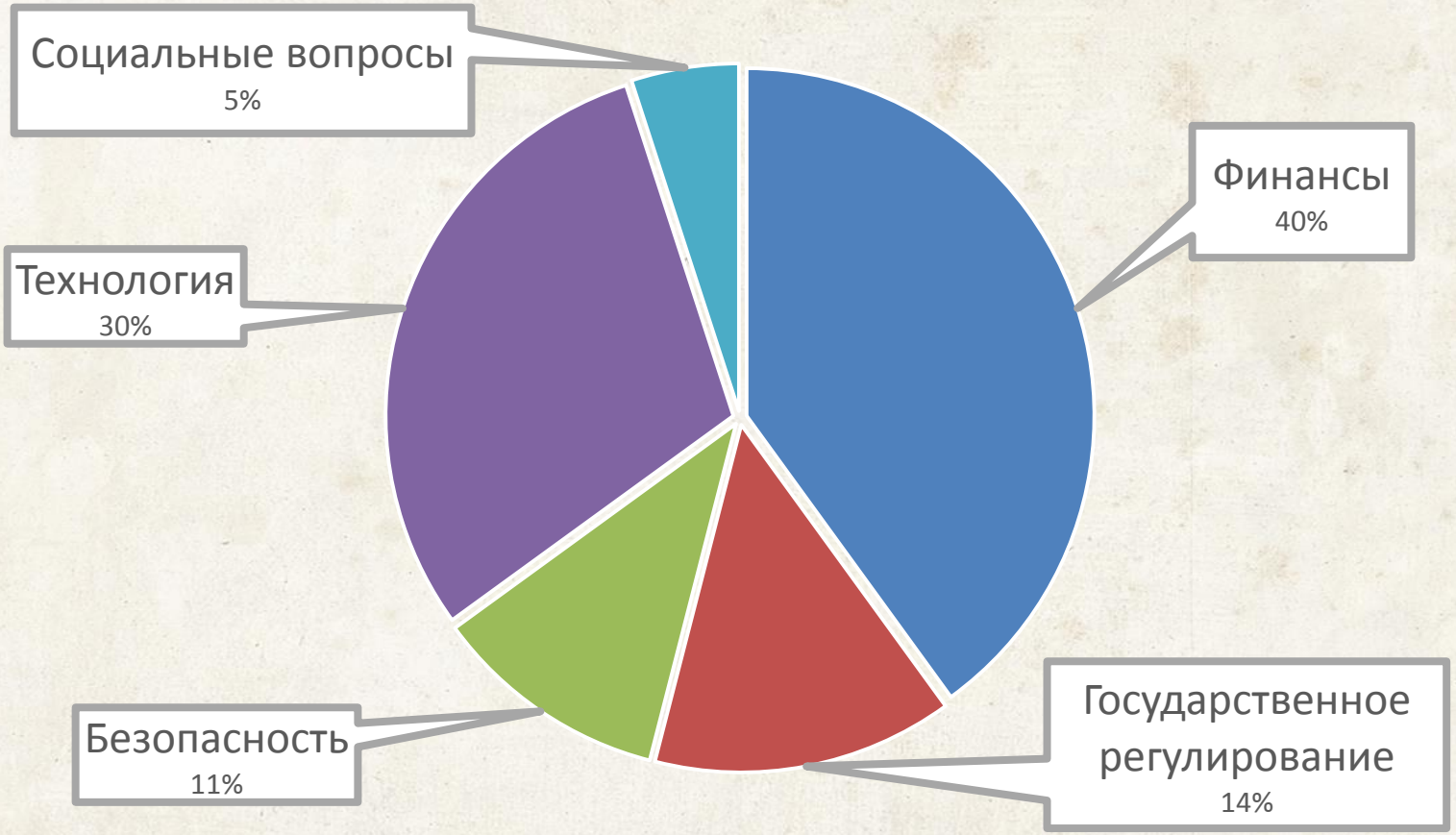
Quantitative Analysis of the Full **Bitcoin** Transaction Graph
https://eprint.iacr.org/2012/584.pdf
File Format: PDF/Adobe Acrobat
a graph of all the **Bitcoin** addresses and transactions up to that date. We then ... analysis of the **Bitcoin** transaction graph was presented at the Chaos Computer.
Labeled ePrint

Two **Bitcoins** at the Price of One? Double-Spending Attacks on Fast ...
https://eprint.iacr.org/2012/248.pdf
File Format: PDF/Adobe Acrobat
detection of double-spending attacks—in which an adversary attempts to use some of her coins for two or more payments. Since **Bitcoin** users are anony-.
Labeled ePrint

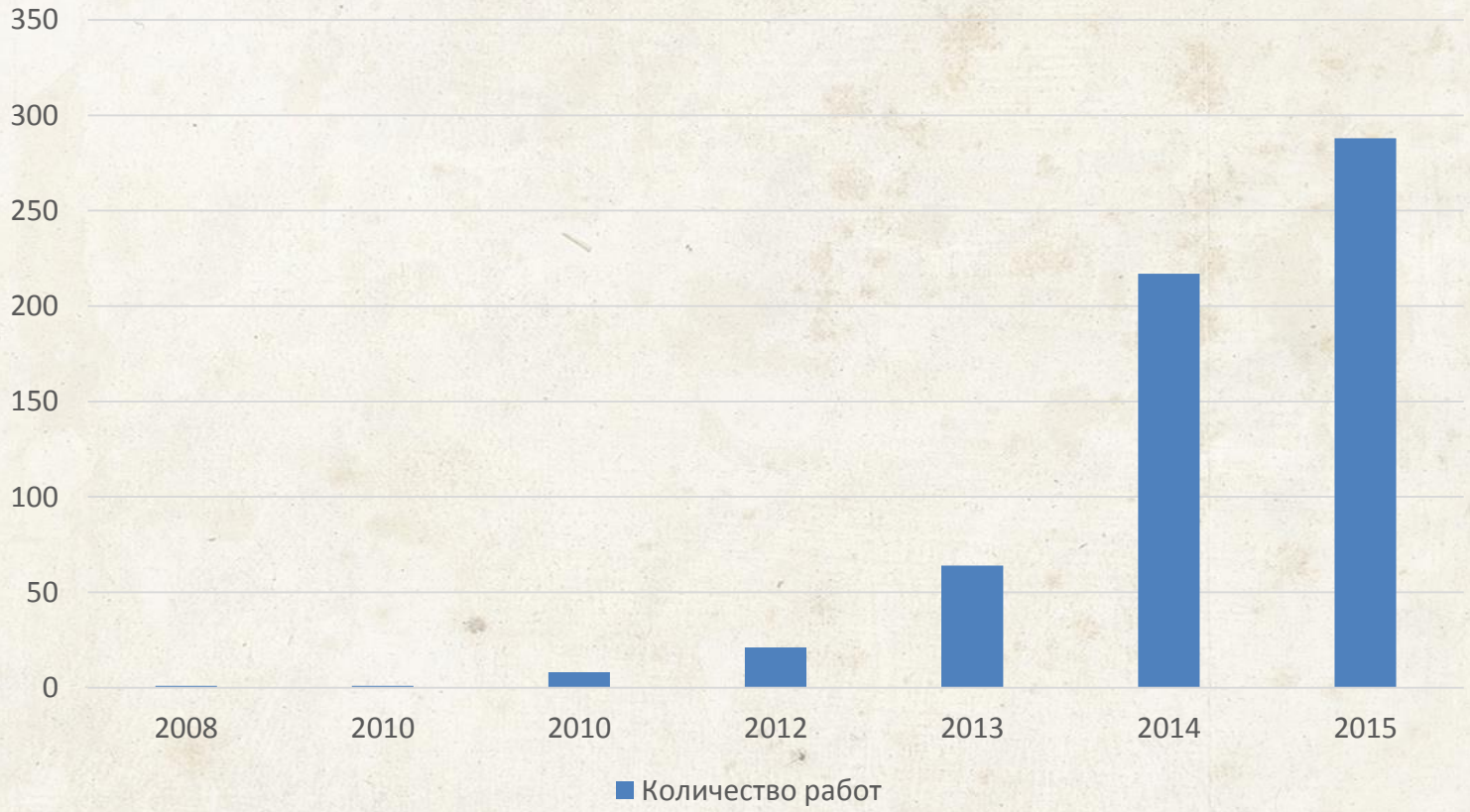
The **Bitcoin** Backbone Protocol: Analysis and Applications*
https://eprint.iacr.org/2014/765.pdf
File Format: PDF/Adobe Acrobat
Jan 27, 2016 ... extract and analyze the core of the **Bitcoin** protocol, which we term the **Bitcoin** ... The public transaction ledger captures the essence of **Bitcoin's** ...
Labeled ePrint

Evaluating User Privacy in **Bitcoin**
https://eprint.iacr.org/2012/596.pdf

Распределение тем научных работ



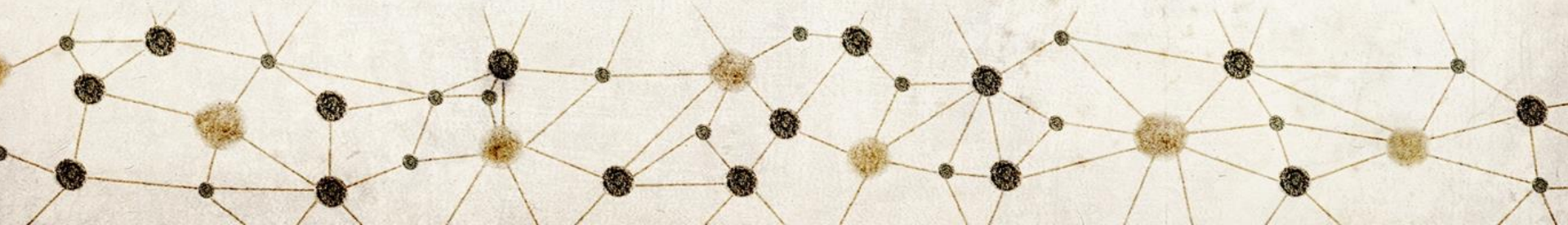
Рост числа новых научных работ по тематике криптовалют



Из истории цифровых наличных денег (digital cash)

Дэвид Ли Чаум (род. 1955) изобретатель многих криптографических проток, а так же ecash и DigiCash. Его работа 1981 года «Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms» заложила основу в области исследования анонимности передаваемых сообщений.

Суть цифровых наличных денег (digital cash)



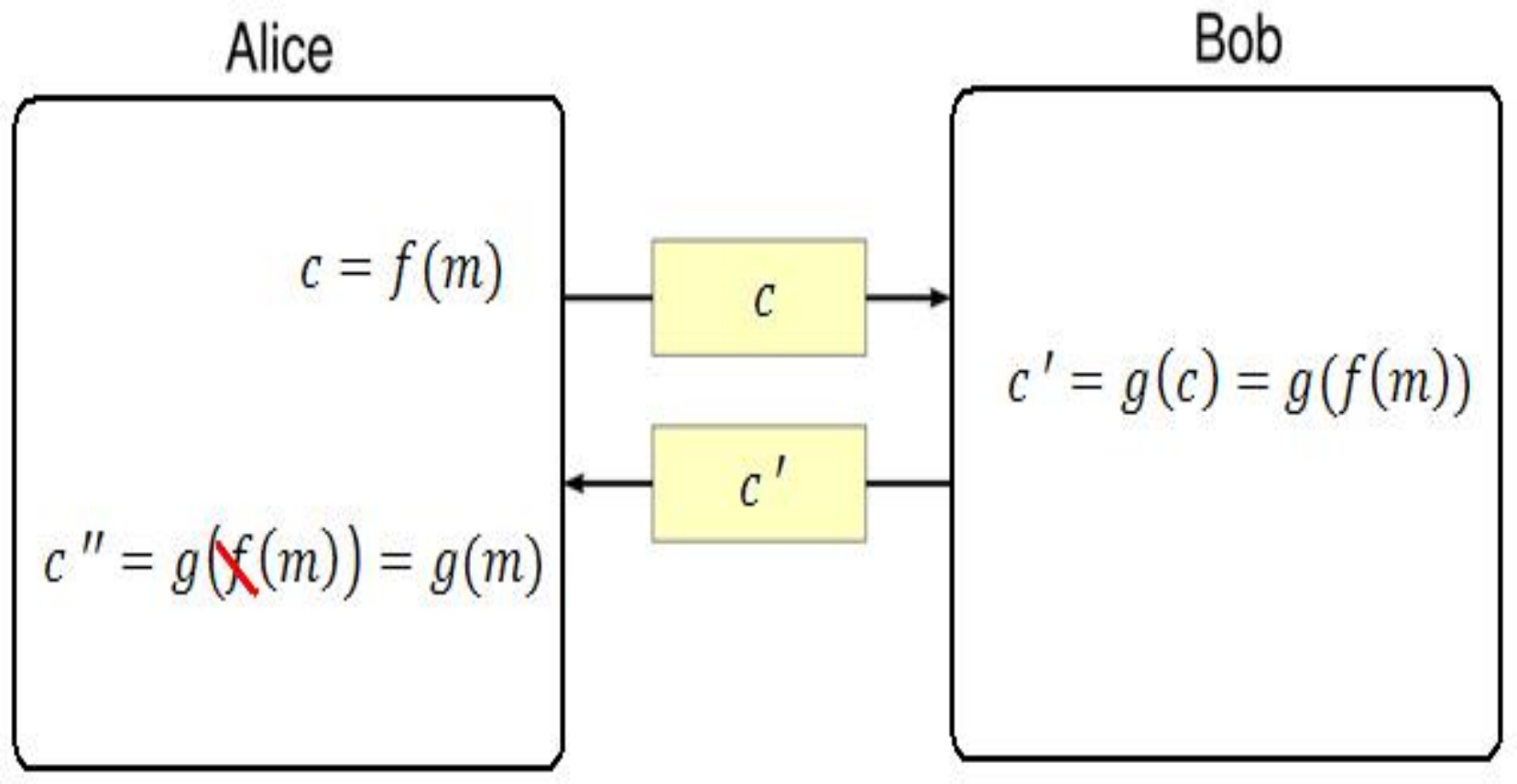
Цифровые наличные деньги (digital cash)
Как это работает

Основная идея слепых подписей заключается в следующем:

1. Отправитель A шифрует документ и посылает его стороне B.
2. Сторона B, не видя содержимое документа, подписывает его и возвращает обратно стороне
3. Сторона A снимает свой шифр, оставляя на документе только подпись стороны B.

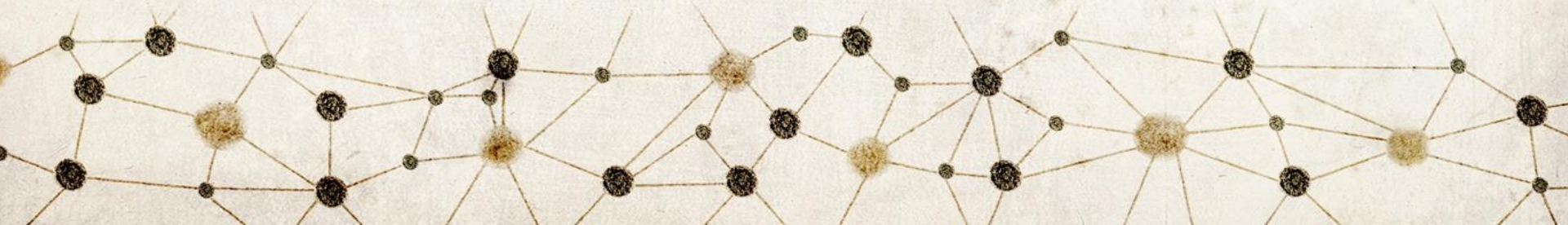
По завершении этого протокола сторона B ничего не знает ни о сообщении t, ни о подписи под этим сообщением.

Цифровые наличные деньги (digital cash)
Полностью слепая подпись



Цифровые наличные деньги (digital cash) Слепая подпись на основе ЭЦП Шнора

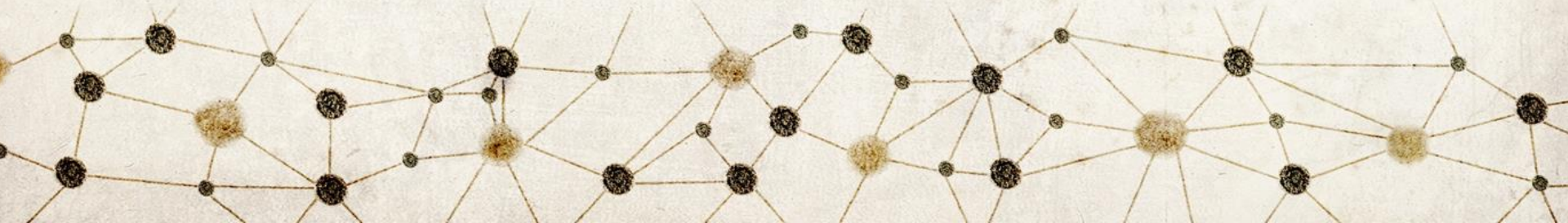
1. Алиса инициирует взаимодействие с Бобом
2. Боб отправляет Алисе значение $R = a^k mod\ p$
3. Алиса вычисляет значение $R^| = Ra^{-\omega}y^{-t} mod\ y$, $E^| = H(\ m||R^|\ )$, $E = E^| + t\ mod\ y$ и отправляет Бобу значение E
4. Боб вычисляет S, такое что $R = a^S y^E mod\ p$ и отправляет S Алисе
5. Алиса вычисляет подпись $(E^|, S^|)$, где $E^| = E^{-t} \mathrm{mod\ y}$ и $S^| = S - \omega mod\ \ y$, которая является подлинно по отношению к сообщению m



Формальное описание

Языком ГОСТ 34 на автоматизированные системы

1. Данные
2. Математическое обеспечение (алгоритмы, форматы)
3. Программное обеспечение
4. Вычислители
5. Каналы передачи данных, сети
6. Люди

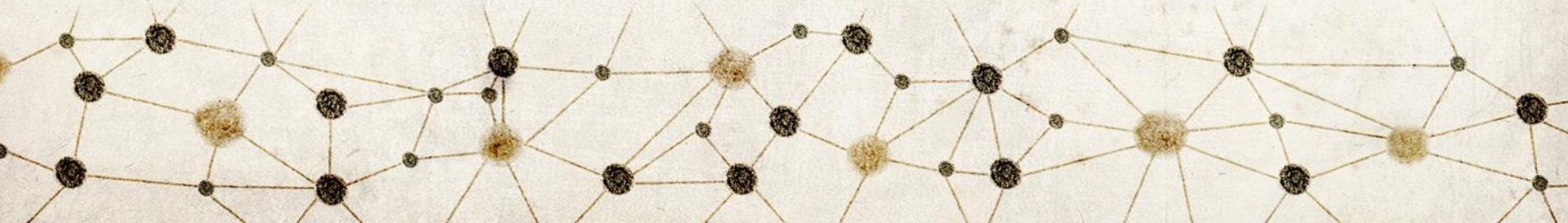


Формальное описание

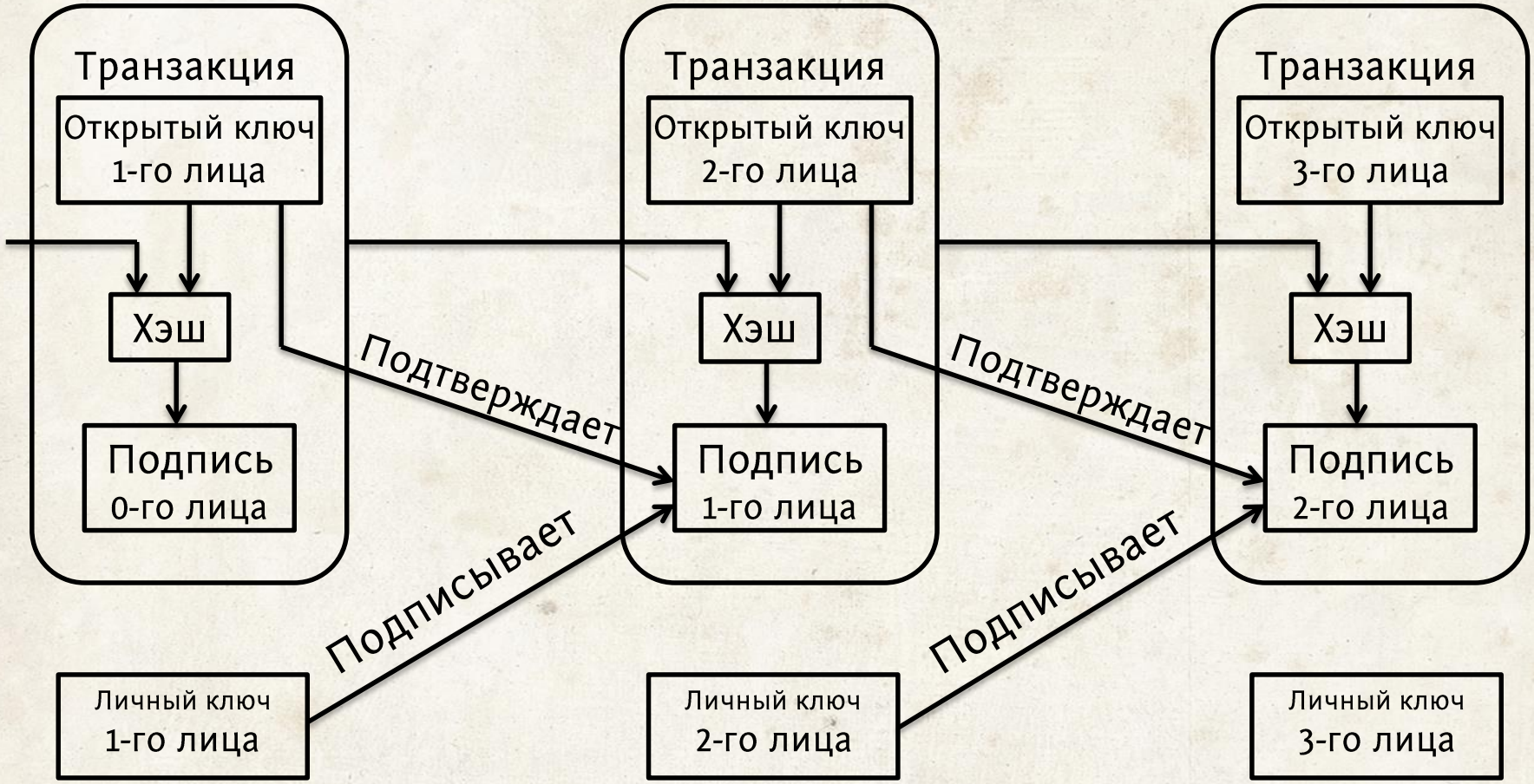
Языком ГОСТ 34 на автоматизированные системы

1. Данные

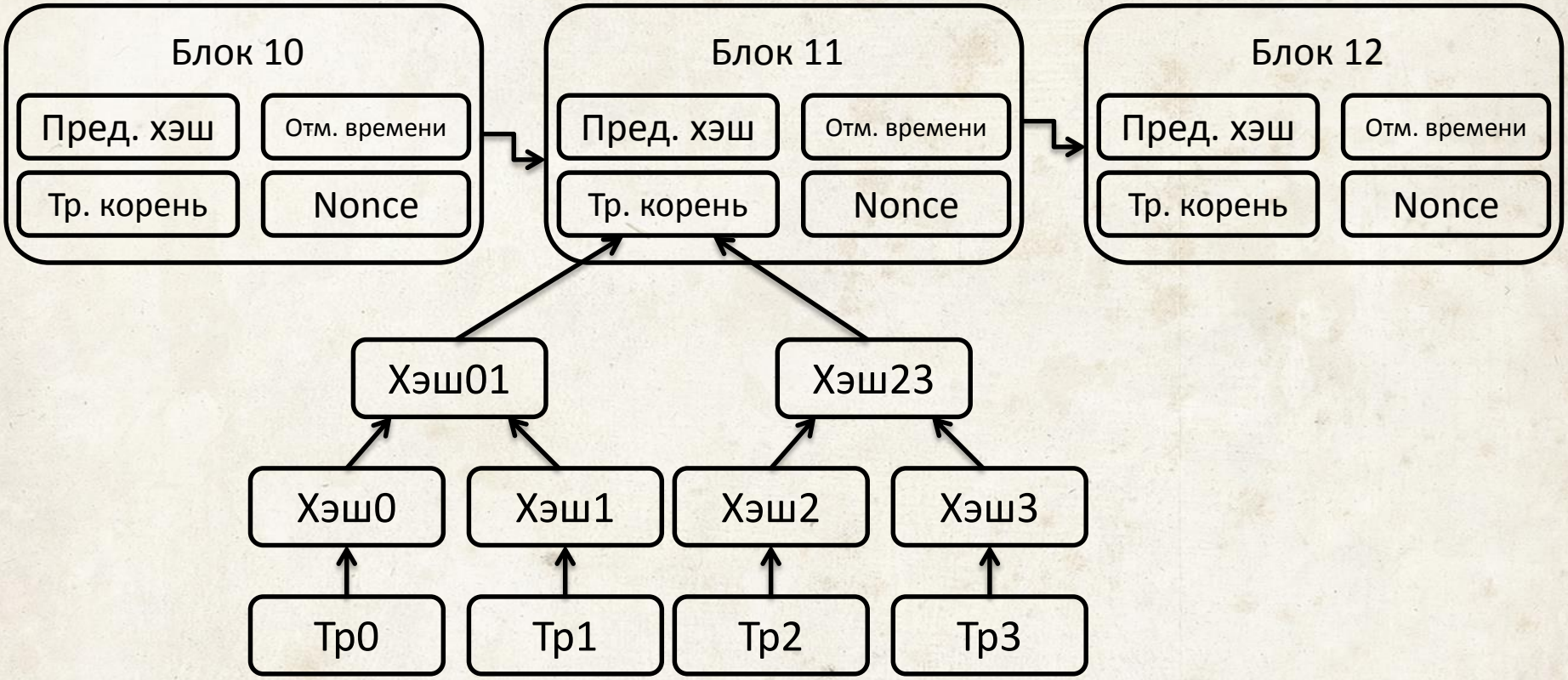
1. Цепочка блоков - набор данных, построенных по определенным правилам, 60 Гб
2. Личные ключи подписи (кошелек)
3. Открытые ключи проверки подписи



Транзакция


Транзакция
Открытый ключ 1-го лица
Хэш
Подпись 0-го лица
Транзакция
Открытый ключ 2-го лица
Хэш
Подпись 1-го лица
Транзакция
Открытый ключ 3-го лица
Хэш
Подпись 2-го лица
Подтверждает
Подтверждает
Подписывает
Подписывает
Личный ключ 1-го лица
Личный ключ 2-го лица
Личный ключ 3-го лица

Блок


Блок 10
Пред. хэш
Отм. времени
Тр. корень
Nonce
Блок 11
Пред. хэш
Отм. времени
Тр. корень
Nonce
Блок 12
Пред. хэш
Отм. времени
Тр. корень
Nonce
Хэш01
Хэш23
Хэш0
Хэш1
Хэш2
Хэш3
Тр0
Тр1
Тр2
Тр3

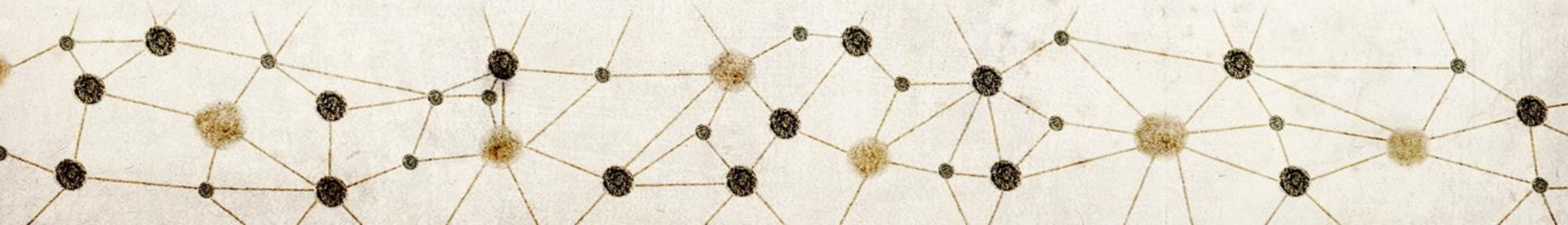
Цепочка блоков

Формальное описание

Языком ГОСТ 34 на автоматизированные системы

2. Математическое обеспечение (алгоритмы, форматы)

1. Алгоритмы ЭЦП
2. Алгоритмы хэширования
3. Форматы



ECDSA

FIPS PUB 186-4

FEDERAL INFORMATION PROCESSING STANDARDS PUBLICATION

Digital Signature Standard (DSS)

CATEGORY: COMPUTER SECURITY **SUBCATEGORY: CRYPTOGRAPHY**

Information Technology Laboratory
National Institute of Standards and Technology
Gaithersburg, MD 20899-8900
http://dx.doi.org/10.6028/NIST.FIPS.186-4
Issued July 2013

U.S. Department of Commerce
Cameron F. Kerry, Acting Secretary
National Institute of Standards and Technology
Patrick D. Gallagher, Under Secretary of Commerce for Standards and Technology and Director

SHA256

FIPS PUB 180-4

FEDERAL INFORMATION PROCESSING STANDARDS PUBLICATION

Secure Hash Standard (SHS)

CATEGORY: COMPUTER SECURITY SUBCATEGORY: CRYPTOGRAPHY

Information Technology Laboratory
National Institute of Standards and Technology
Gaithersburg, MD 20899-8900

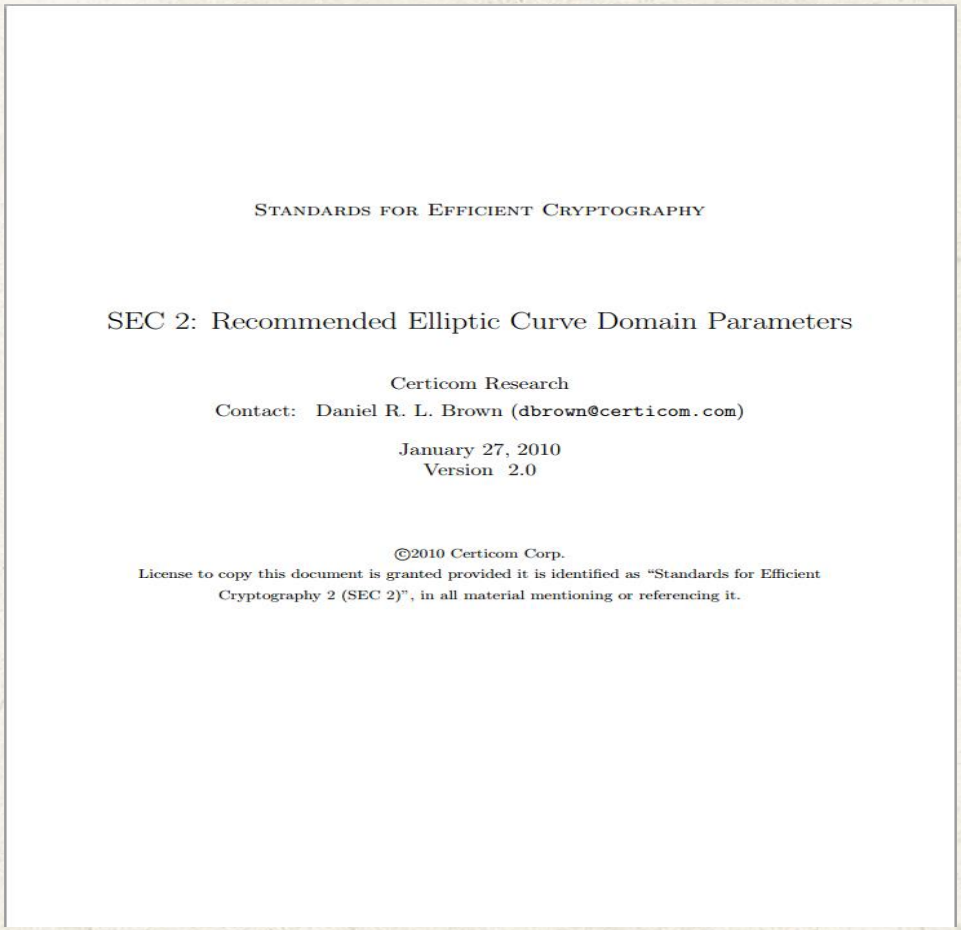
This publication is available free of charge from:
http://dx.doi.org/10.6028/NIST.FIPS.180-4

August 2015

U.S. Department of Commerce
Penny Pritzker, Secretary

National Institute of Standards and Technology
Willie E. May, Under Secretary for Standards and Technology and Director

sec256k1



STANDARDS FOR EFFICIENT CRYPTOGRAPHY

SEC 2: Recommended Elliptic Curve Domain Parameters

Certicom Research
Contact: Daniel R. L. Brown (dbrown@certicom.com)

January 27, 2010
Version 2.0

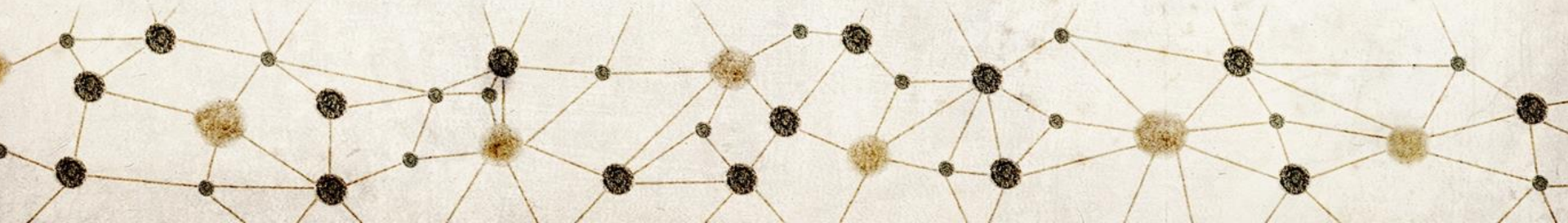
Формальное описание

Языком ГОСТ 34 на автоматизированные системы

3. Программное обеспечение

Программный комплекс:

1. Клиентское ПО
2. ПО узлов (реализует распределенные вычисления по решению задачи закрепления блока)

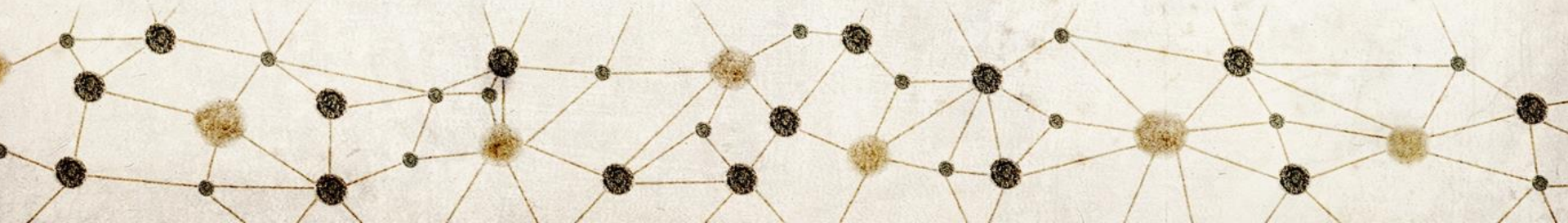


Формальное описание

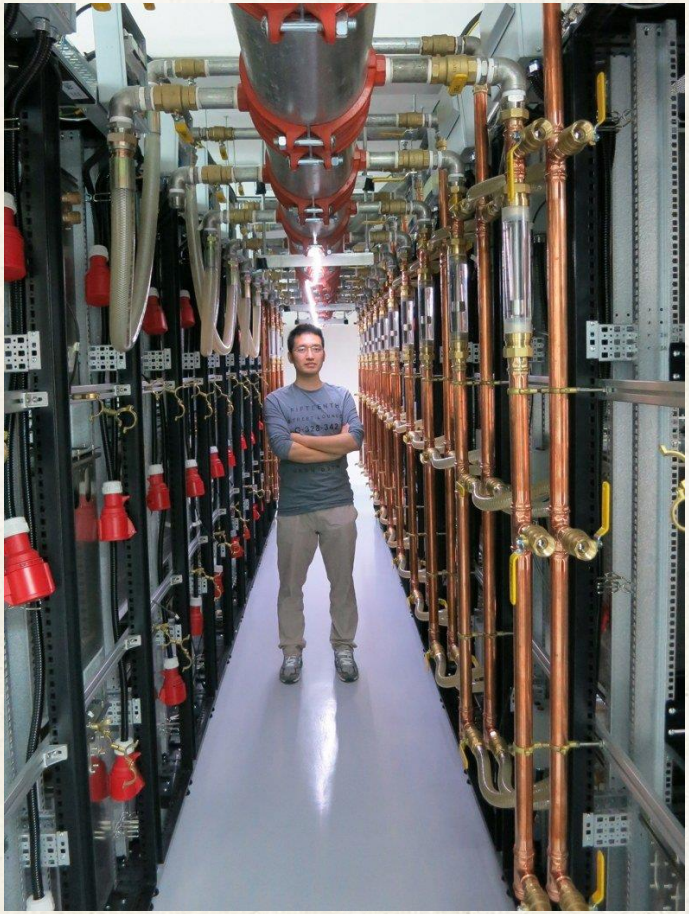
Языком ГОСТ 34 на автоматизированные системы

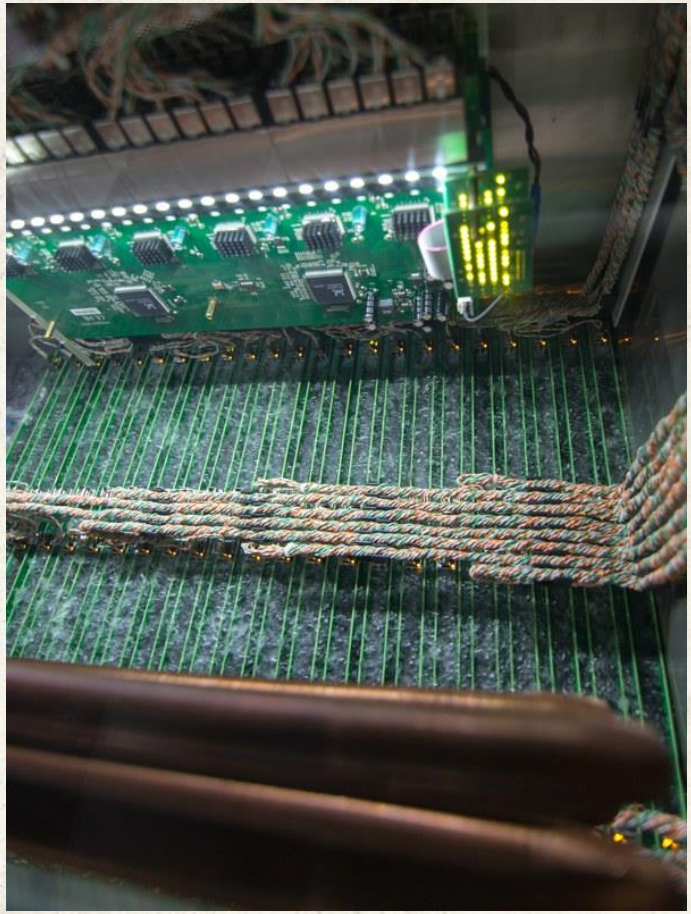
4. Вычислители

1. Персональные компьютеры
2. Сервера
3. Суперкомпьютеры
4. Фермы



Фермы



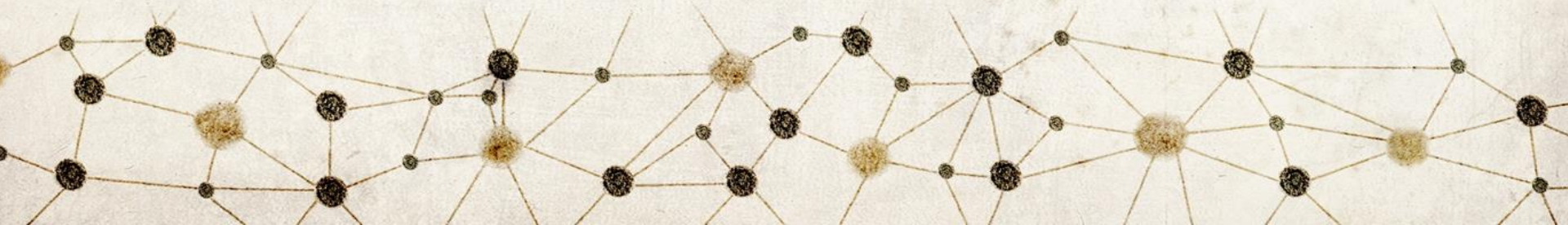


Формальное описание

Языком ГОСТ 34 на автоматизированные системы

5. Каналы передачи данных, сети

Одноранго́вая, децентрализо́ванная или пи́ринговая (англ. peer-to-peer, P2P — равный к равному) сеть — это оверлейная компьютерная сеть, основанная на равноправии участников. Часто в такой сети отсутствуют выделенные серверы, а каждый узел (peer) является как клиентом, так и выполняет функции сервера. В отличие от архитектуры клиент-сервера, такая организация позволяет сохранять работоспособность сети при любом количестве и любом сочетании доступных узлов. Участниками сети являются пиры.

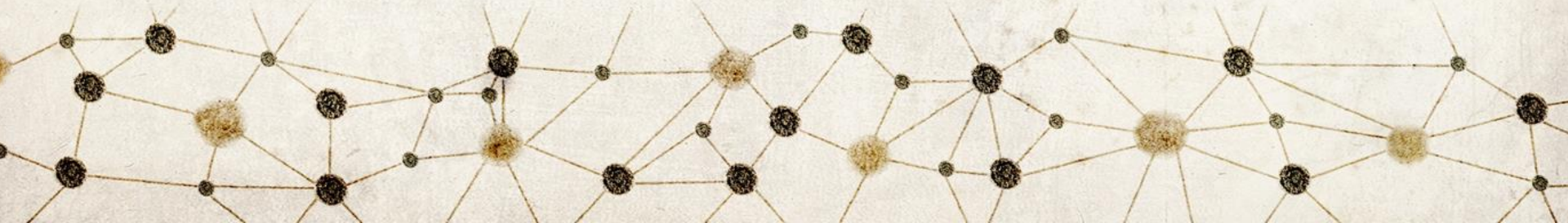


Формальное описание

Языком ГОСТ 34 на автоматизированные системы

6. Люди

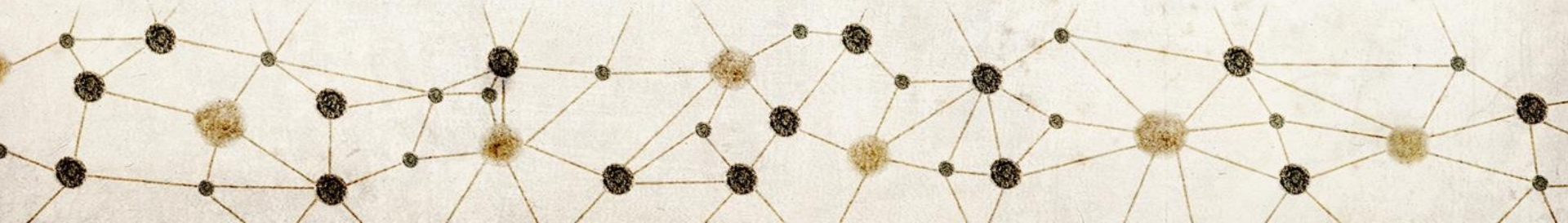
Пользователь системы – человек, установивший ПО и получивший возможность распоряжаться учетными единицами. Тот, у кого имеется личный ключ, на открытый ключ которого передана возможность воспользоваться у.е. Те, у кого такого нет – не пользователи



Угрозы, атаки, модель нарушителя

Завладеть личным ключом, на котором есть биткоины:

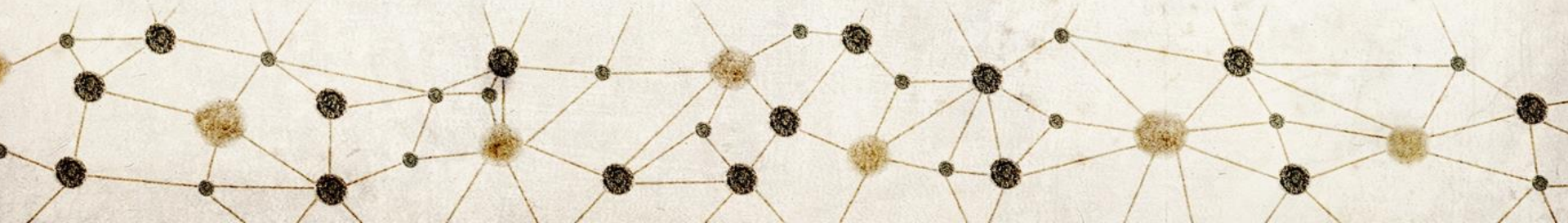
1. Похитить (защита кошелька)
2. Найти по открытому ключу (логарифмирование в группе точек эллиптических кривых)



Угрозы, атаки, модель нарушителя

Не зная личный ключ, получить возможность распоряжаться биткоинами (получить биткоины на свой кошелек)

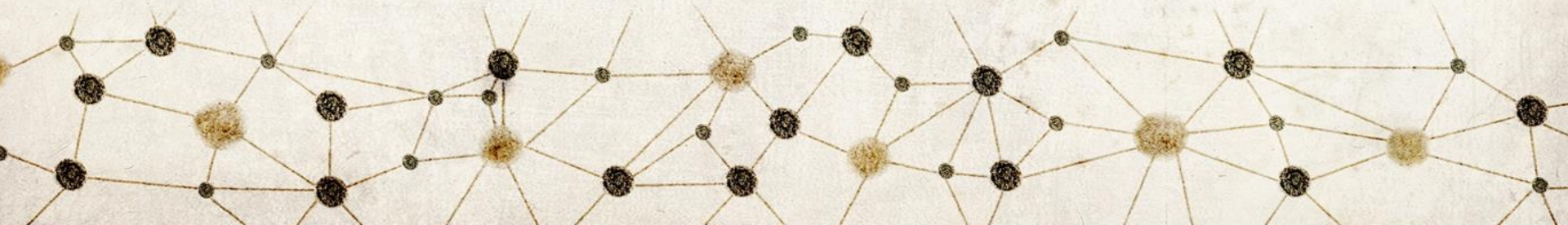
1. Взом блокчейн. Изменить уже закрепленную транзакцию, так чтобы получить возможность распоряжаться биткоинами на свой открытый ключ. Изменить транзакцию из блокчейн так, чтобы биткоины попали на открытый ключ мошенника с закреплением блока, легально в смысле в системы.



Угрозы, атаки, модель нарушителя

Не зная личный ключ, получить возможность распоряжаться коинами (получить биткоины на свой кошелек)

2. Без взлома существующей блокчейн. Сформировать подписанную транзакцию так, чтобы она проверялась открытым ключом владельца и перечислить биткоины в этой транзакции на свой (мошенника) ключ. Создать транзакцию, передающую возможность использования биткоинов на свой кошелек и выставить ее на закрепление. Тут мало того, что нужно сформировать легальную транзакцию по правилам системы, так ее нужно еще закрепить.



Задача создания блока

h – хэш-функция, являющаяся композицией двух sha256

t – цель (в битовом представлении имеет серию нулей в старших разрядах)

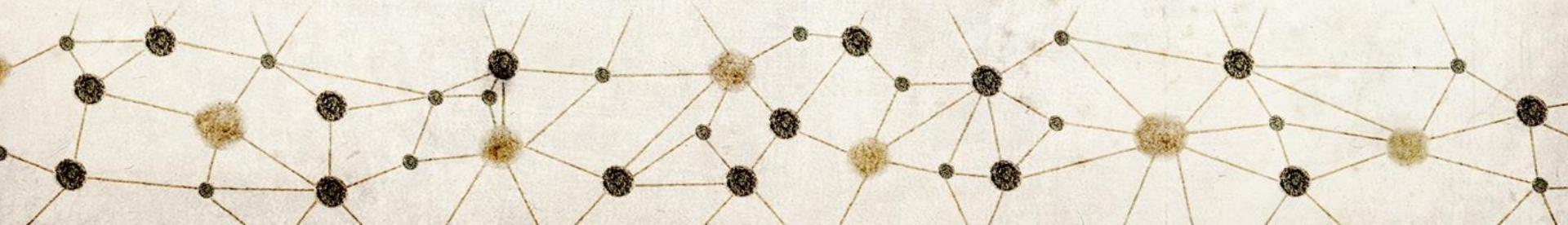
d – служебные данные (заголовок блока, хэши транзакций и прочее)

Задача получения блока:

Для фиксированных: t из Z_{256}, натурального n, d из V_n

Найти x из V_{256}, такой что

$$h(d||x) < t$$



Задача создания блока

h – хэш-функция, являющаяся композицией двух sha256

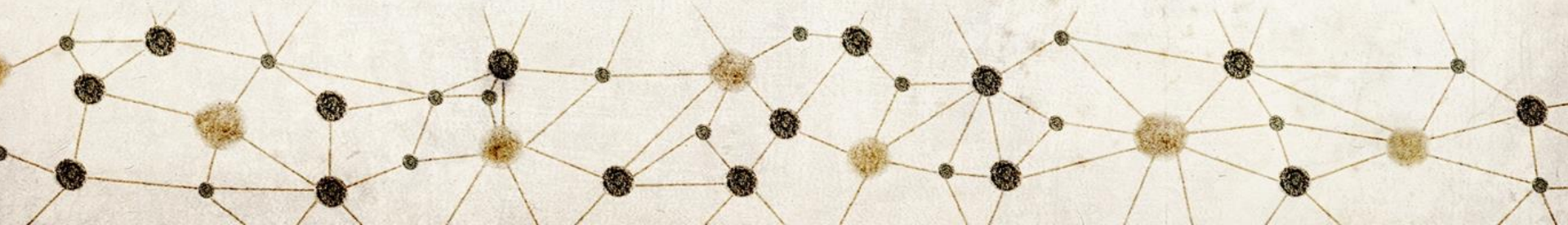
t – цель (в битовом представлении имеет серию нулей в старших разрядах)

d – служебные данные (заголовок блока, хэши транзакций и прочее)

Известный и широко используемый метод решения (переборный):

Последовательно перебирая (случайно выбирая) x из V_{256} найти такой, что

$$h(d||x) < t$$



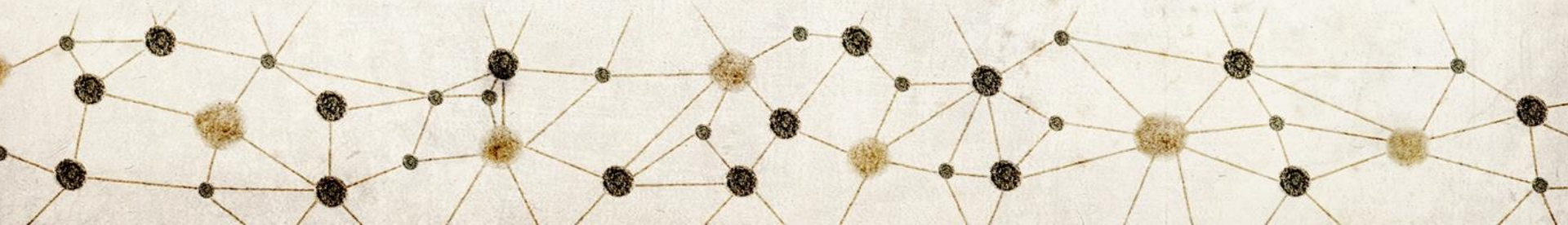
Задача создания блока

Можно посмотреть на эту задачу и по-другому:

Для фиксированных: t из Z_{256}, натурального n, d из V_n

Найти пару (x,y), где x из V_{256}, y из Z_{256} и $y < t$, такую что

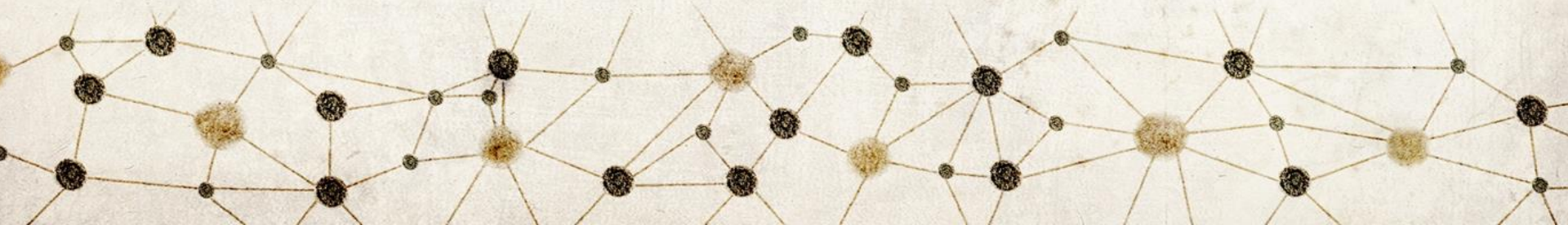
$$h(d||x)=y$$



Связь со стойкостью функций хэширования, оценка взаимосвязи задач:

Для $h_d : Z_{256} \to Z_t$ (Z_t множество целых, меньших чем t) найти произвольные аргумент и соответствующее ему значение

Найти алгоритм со сложностью меньшей чем сложность метода перебора или случайного поиска



Угрозы, атаки, модель нарушителя Не криптографические

1. отказ в обслуживании, а именно направление в систему большого количества транзакций с совершением переводов на ничто мало количество единиц. Таких транзакций направляется очень много и время обычной обработки транзакции с 10 минут поднимается до 14 часов.

2. выявление людей, которые проводят транзакции, т.к. изначально можно зафиксировать откуда пошёл первый сигнал о транзакции и после этого найти адрес первого отправителя – разбор путей передачи на основании данных о сетях

3. вредоносное ПО, которое заставляет заниматься майнингом другие вычислители на кошелек мошенника

On Bitcoin Security in the Presence of Broken Crypto Primitives

February 19, 2016

Ilias Giechaskiel
University of Oxford
Oxford, United Kingdom
ilias.giechaskiel@cs.ox.ac.uk

Cas Cremers
University of Oxford
Oxford, United Kingdom
cas.cremers@cs.ox.ac.uk

Kasper B. Rasmussen
University of Oxford
Oxford, United Kingdom
kasper.rasmussen@cs.ox.ac.uk

Abstract

Digital currencies like Bitcoin rely on cryptographic primitives to operate. However, past experience shows that cryptographic primitives do not last forever: increased computational power and advanced cryptanalysis cause primitives to break frequently, and motivate the development of new ones. It is therefore crucial for maintaining trust in a crypto currency to anticipate such breakage.

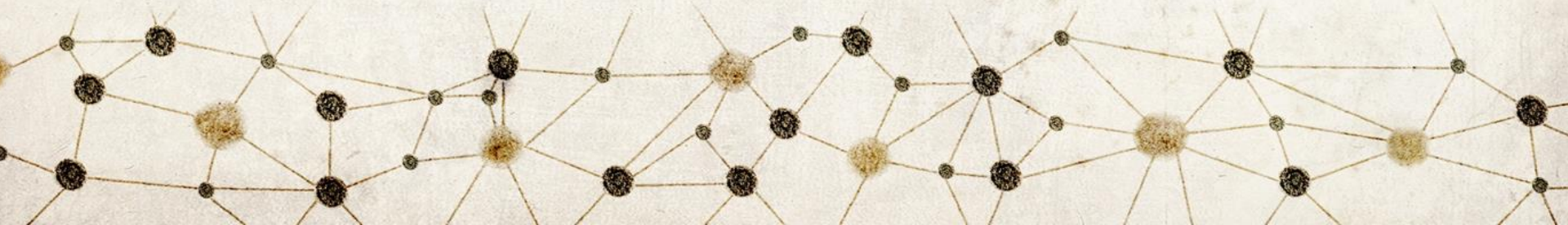
We present the first systematic analysis of the effect of broken primitives on Bitcoin. We identify the core cryptographic building blocks and analyze the various ways in which they can break, and the subsequent effect on the main Bitcoin security guarantees. Our analysis reveals a wide range of possible effects depending on the primitive and type of breakage, ranging from minor privacy violations to a complete breakdown of the currency.

Our results lead to several observations on, and suggestions for, the Bitcoin migration plans in case of broken not fully explained. Moreover, the subsequent steps after a contingency are hand-wavy and incomplete, e.g., "once the plans themselves are well-accepted, code implementing the plans can be written and tested in case the code is ever required" [11]. To the best of our knowledge, no adequate mechanism has been built into Bitcoin, and no plans for partial breakage (or weakening of a primitive) have been considered.

In practice, the situation is not black-and-white. Instead of abruptly breaking completely, cryptographic primitives usually break gradually. With hash functions, for example, it is common that first a single collision is found. This is then later generalized to multiple collisions, and only later do arbitrary collisions become feasible to compute. In parallel, the complexity of attacks (such as collisions) decreases to less-than-brute-force, and computational power increases. Finally, quantum computing will make some attacks easier, e.g., Grover's pre-image attack [23], or Shor's algorithm for discrete log computation [45].

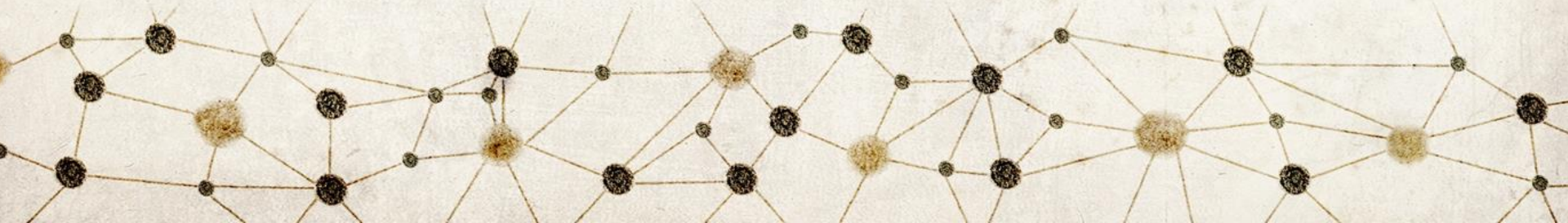
4 Broken Hashing Primitives

In this section, we look at the cryptographic hash functions in Bitcoin, and analyze the effect of a break in one of the properties of first and second pre-image and collision resistance. We generalize these into a single property called chosen-format bounded pre-image resistance.



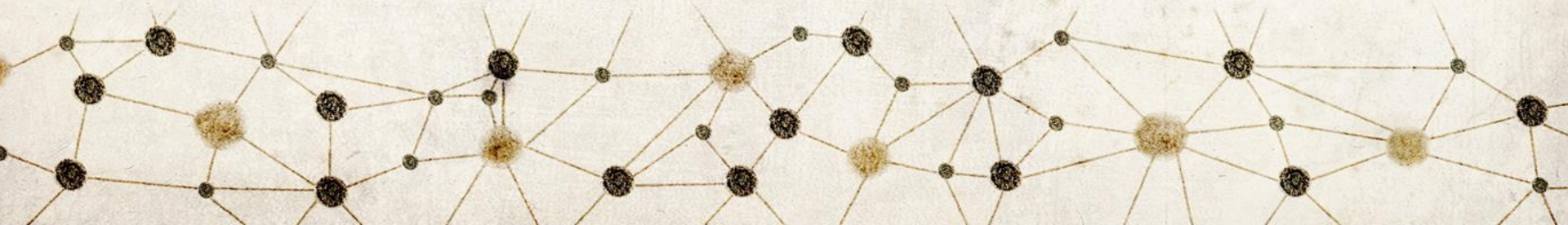
Breakage	**Address Hash (H_A)**	**Main Hash (H_M)**
Collision	Repudiate payment	Destroy coins
Second pre-image	Repudiate payment	Double spend and steal coins
Pre-image	Uncover address	Complete failure of the blockchain ($2n$ calls)
Bounded pre-image	All of the above	Complete failure of the blockchain (n calls)

Table 1: Summary of the effects on Bitcoin for different types of breakage in the two hash functions used.



Breakage	**Effect**
Selective forgery	Steal coins from public key
Integrity break	Claim payment not received
Repudiation	-

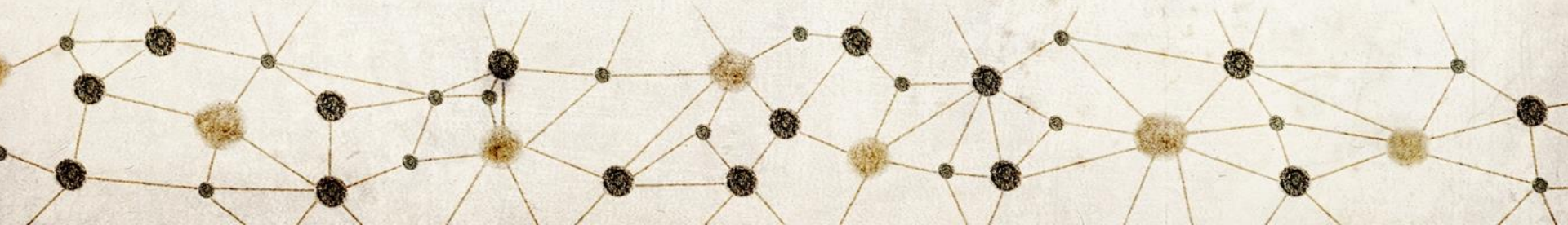
Table 2: Effects of a break in the signature scheme.



	Signature Property		
Hash Property	**Selective forgery**	**Integrity break**	**Repudiation**
Address Hash (H_A)			
Collision	Repudiate transaction	-	Change existing payment†
Second pre-image	Steal all coins	-	Change existing payment
Pre-image	Steal all coins	-	-
Bounded pre-image	All of the above	-	Change existing payment
Main Hash (H_M)			
Collision	Steal coins	Steal coins†	-
Second pre-image	Steal coins	Double spend†	-
Pre-image	-	-	-
Bounded pre-image	Steal coins	All of the above	-

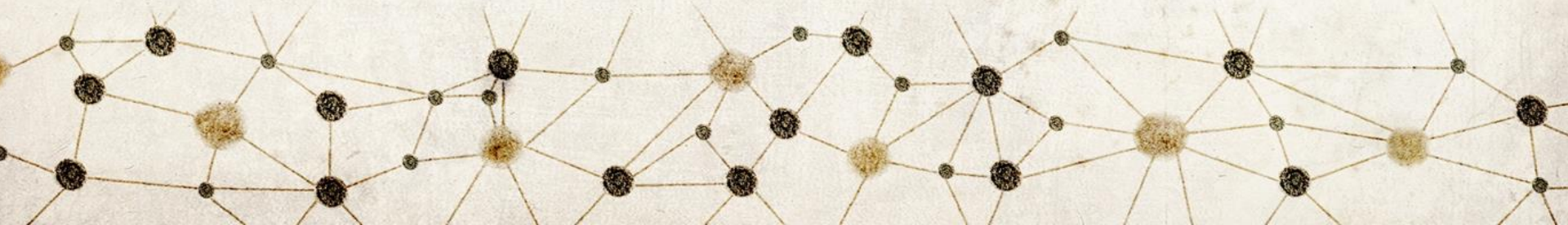
† Achieving this requires a slight modification of the definitions. See text for details.

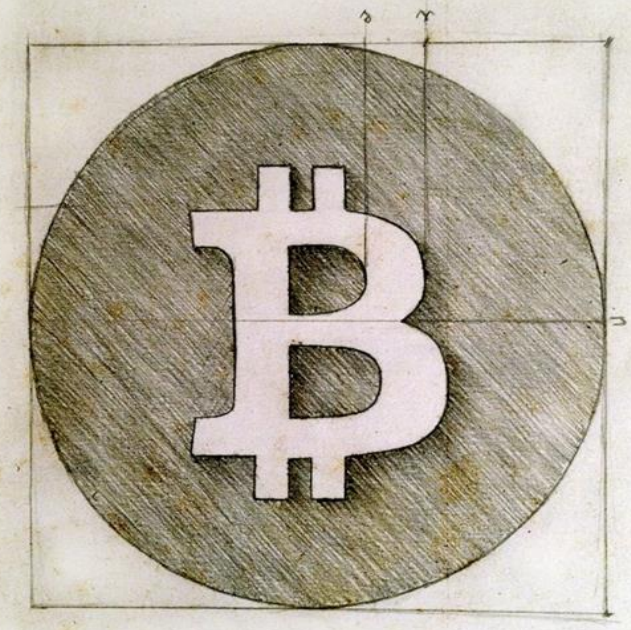
Table 3: The effects of a multi-breakage: broken signature scheme in combination with a break in H_A or H_M.



Breakage	Effect
SHA256	
Collisions	Steal coins
Second pre-image	Double spend
Pre-image	Complete failure
Bounded pre-image	All of the above
RIPEMD160	
Any of the above	Repudiate payments
ECDSA	
Selective forgery	Steal coins, Send fake alerts
Integrity break	Claim payment not received
Repudiation	Send fake alerts

Table 4: Effects of concrete primitive breakage on the current version of Bitcoin.





Спасибо за внимание!

Комисаренко В.В. - 229tut@gmail.com
Роговой А.С. - 83217un@gmail.com