Автор:
27.02.18 22:57 -

1.1 , Аноним , 09:46, 28/02/2018 [ответить] [смотреть все] + / – И все самодельные серты от домашнего уц тоже надо будет туда отправлять?

2.7 , Аноним , 09:59, 28/02/2018 [^] [
ответить
смотреть все
показать ветку
+
–
Нет, надо удалить Chrome.

3.8 , Майнер , 10:02, 28/02/2018 [^] [
ответить
смотреть все
+
–
И установить Firefox на предприятия с Active Directory и стюардессами!

3.9 , Майнер , 10:06, 28/02/2018 [^] [ответить] [смотреть все] +1 + / – https wiki mozilla org Deployment Deploying_Firefox https www mozilla org en...
весь текст скрыт
[
показать
]
4.18
Anonymoustus
^
ответить
смотреть все
+
–
Да-да, и с навечно отключённым жабоскриптом.

3.56 , rvs2016 , 16:02, 28/02/2018 [^] [ответить] [смотреть все] +1 + / – Не поможет Это даст лишь временную передышку, ибо шизофрения в этой теме - зара...
весь текст скрыт
[
показать
]
4.66
гы
^
ответить
смотреть все

+
–
Ничего не изменится. Сложности для разработчиков сайтов только прибавилось чуток...
Большинство и не юзало ваши фидонеты никогда. А меньшинство продолжает юзать что-то под
Когда большинство освоило пк на уровне "выйти в интернет" им уже надо было конкрентно откр

2.20 , Аноним , 11:15, 28/02/2018 [^] [ответить] [смотреть все] [показать ветку] +
6
+
/
–
Let's Encrypt изначально логи Certificate Transparency поддерживает.
2.33 , Аноним , 12:49, 28/02/2018 [^] [ответить] [смотреть все] [показать ветку] +3
+
/
–
2.53
,
Аноним
, 15:12, 28/02/2018 [
^
] [
ответить
] [
смотреть все
] [
показать ветку
]
+2
+
/
–
2.57
,
rvs2016
, 16:03, 28/02/2018 [
^
] [
ответить
] [
смотреть все
] [
показать ветку
]
+1

Автор:
27.02.18 22:57 -

+
/
–
> Гугл - чудаки.

Не то слово! Но более важная проблема в том, что они такие не одни. За ними последуют и остальные! И тогда наступит полный каюк! Беспрепятственного доступа к информации в WWW больше не будет!

3.60 , Anonim 2.0 , 16:35, 28/02/2018 [^] [ответить
смотреть все
+
–
И грядет конец света! Истинно говоря я Вам !!!

3.67 , гы , 17:53, 28/02/2018 [^] [ответить] [смотреть все] + / – >> Гугл - чудаки.
> Не то слово! Но более важная проблема в том, что они такие
> не одни. За ними последуют и остальные! И тогда наступит полный
> каюк! Беспрепятственного доступа к информации в WWW больше не будет!

Если кто-то сможет самолично удалять сертификаты из списка, то это будет контроль за распространением инфы, а если не сможет (хотя бы восприпятствовать занесению твоего сертификата в список), то ничего не изменится.

1.3 , Аноним , 09:52, 28/02/2018 [ответить] [смотреть все] +1 + / – А доступ к CT? По Https? :)
1.4 , Аноним , 09:55, 28/02/2018 [ответить] [смотреть все] –1 + / – IP клиента анонима при заходе на HTTPS 1 0-1 1 и HTTP 2 0 сайты тоже будет запис...
весь текст скрыт
[
показать
]

2.27
Аноним
^
ответить
смотреть все
показать ветку
+
–

4.77 , Аноним , 22:49, 28/02/20
^
ответить
смотреть все
к модератору
+
–
Ща Мишаня придёт и деонанирует нас всех.

4.78 , Аноним , 23:01, 28/02/2018 [^] [ответить] [смотреть все] [к модератору] + / –
Виктор Феофанов, Санкт-Петербург, 207 школа, 9а класс Сидишь под дебианом, fire...
весь текст скрыт
[
показать
]
5.81
Аноним
^
ответить
смотреть все
к модератору
+
–
Мимо Мимо Мимо Поэтому такая соль в том, что анонимность разлагает Неко...
весь текст скрыт [показать]

1.5 , Аноним , 09:58, 28/02/2018 [ответить] [смотреть все] +1 + / – надо же, полный абзац вместо бузворда "блокчейн"

2.11 , Аноним , 10:06, 28/02/2018 [^] [
ответить
смотреть все
показать ветку
+
–
Я считаю, что hashmap - это блокчейн. Сатоси Накамото - гений.

3.14 , тоже Аноним , 11:01, 28/02/2018 [^] [
ответить
смотреть все
+
–
Вы можете считать, что весь текст скрыт в абзаце, насколько я вижу, описываемый блок...
весь текст скрыт [показать]

4.17 , Аноним , 11:05, 28/02/2018 [^] [

ответить
смотреть все
+
–
В mercurial тоже описан блокчейн, не линейный, а древовидный. Или нет?

4.42 , DFgertert , 13:20, 28/02/2018 [^] [ответить] [смотреть все] + / – Сэр, почитайте про блокчейн, в нем ничего суперинновационного нет, технологии ст...
весь текст скрыт
[
показать
]
4.45
,
Crazy Alex
, 13:29, 28/02/2018 [
^
] [
ответить
] [
смотреть все
]
+1
+
/
–
Блокчейн без блоков?

5.49 , тоже Аноним , 14:31, 28/02/2018 [^] [
ответить
смотреть все
+
–
Если частью каждой записи является хэш предыдущей записи, то эта запись - блок блокчейна. Я не прав?

6.58 , Аноним , 16:17, 28/02/2018 [^] [
ответить
смотреть все
+
–
Нет, просто запись содержит часть предыдущей записи.

7.62 , тоже Аноним , 16:52, 28/02/2018 [^] [

Автор:
27.02.18 22:57 -

ответить
смотреть все
+
–
О учитель! Я, позднорожденный, безрассуден и глуп.
Укажи же мне это критичное отличие, которого мои старые и слабые глаза не могут увидеть.

6.63 , Crazy Alex , 17:00, 28/02/2018 [^] [ответить] [смотреть все] + / – Разве что в очень вырожденном виде. По-хорошему блокчейн подразумевает именно группировку записей в блоки с фиксированным максимальным размером и генерацию этих блоков с более-менее постоянной скоростью независимо от наличия в них содержимого. Я не готов внятно объяснять, что это даёт, но если невнятно - то так обеспечивается хоть как-то предсказуемый таймстампинг и куча разных дополнительных валидаций начиная с банальной защиты от спама.

7.64 , тоже Аноним , 17:17, 28/02/2018 [^] [
ответить
смотреть все
+
–
Я так понимаю, что записи в обсуждаемом дереве как раз должны вписываться в фиксированн
А вот зачем блокчейну генерить пустые блоки, если в него и так поток будет идти постоянно - им

8.79 , Crazy Alex , 00:05, 01/03/2018 [^] [
ответить
смотреть все
к модератору
+
–
Фиксированный размер - имеется в виду фиксированный максимальный размер блока. Пустые б

1.6 , Майнер , 09:59, 28/02/2018 [ответить] [смотреть все] –3 + / – так и пишите подобно смарт-контрактам...
весь текст скрыт
[
показать
]

2.10
Ан
^
ответить
смотреть все
показать ветку

+
–
тогда уже блокчейну. Смарт контракт это о другом.

2.28 , Аноним , 12:39, 28/02/2018 [^] [ответить] [смотреть все] [показать ветку] +1 +
/
–
Торент файлы использовали эту структуру задолго до.
2.55 , Аноним , 15:38, 28/02/2018 [^] [ответить] [смотреть все] [показать ветку] +1
+
/
–

1.12
,
Аноним
, 10:12, 28/02/2018 [
ответить
] [
смотреть все
]
–3
+
/
–
я хоть и ярый фанатик гугла, но даже я чутка возмущен
2.29 , Аноним , 12:41, 28/02/2018 [^] [
ответить
смотреть все
показать ветку
+
–
> я хоть и ярый фанатик гугла, но даже я чутка возмущен

Чем? Тем что китайские удостоверяющие центы не смогут продавать на черном рынке валидные

3.70 , нах , 19:11, 28/02/2018 [^] [
ответить
смотреть все
+
–
и некитайские на белом тоже не смогут - потому что мало поклониться в ноженьки владельцам

Ну, разумеется же, для того чтоб каждый юзер мог убедиться...стоп-стоп-стоп...какой юзер, чего

there should be only ONE.

4.74 , Аноним , 20:41, 28/02/2018 [^] [ответить смотреть все + –

CAN be only one Если не хочешь скрывать гугла и не выражаешь сочувствие [показать] личное...

1.13 , ойой , 10:42, 28/02/2018 [ответить] [смотреть все] +2 + / – Я правильно понял, что новость касается только удостоверяющих центров, которые выпускают сертификаты, и они сами будут информировать CT о выпусках?
Т.е. конечного владельца сертификата это мало должно волновать?

2.15 , тоже Аноним , 11:04, 28/02/2018 [^] [ответить смотреть все показать ветку + –

Да, пока все идет, как задумано. Задумано, что теперь для подделки сертификата н... [показать] [показать ветку

3.34 , Аноним , 12:49, 28/02/2018 [^] [ответить смотреть все + –

Публичный лог нужен не только для выпуска сертификата от другого CA, ... [показать]

4.38 , Аноним , 13:07, 28/02/2018 [^] [ответить смотреть все + –

Что не как не помешает тому CA что выдал ваш сертификат, распространить его поба... [показать]

5.50 , Аноним , 15:03, 28/02/2018 [^] [ответить

Автор:
27.02.18 22:57 -

смотреть все
+
–
Побайтовые копии даже сейчас никто не может распространять Приватный ключ серти...
весь текст скрыт
[
показать
]

5.68 , Тузя , 18:14, 28/02/2018 [^] [ответить] [смотреть все] –1 + / – А какое отношение инфраструктура PKI имеет к понятию безопасность Когда незнако...
весь текст скрыт
[
показать
]
6.76
Аноним
^
ответить
смотреть все
к модератору
+
–
> не отличает туалетную бумагу "страховай полис" от криптографических гарантий

6.80 , Crazy Alex , 00:14, 01/03/2018 [^] [ответить] [смотреть все] [к модератору] + / –
В большинстве случаев (в интернете) вообще наплевать, какое там лицо или совсем даже морда. А важно:
1) чтобы ты в следующий раз общался с тем же лицом
2) чтобы, придя по ссылке, о которой где-то в доверенном источнике узнал, ты попал именно туда, а не к левому дяде
3) чтобы ваш обмен данными не подменил левый хрен.

Причём всё это не на уровне "шпионских игр", а вполне себе обычных задач - пообщаться со знакомыми, купить что-то в интернет-магазине и оплатить покупку, оставить резюме у потенциального работодателя и так далее.

Вот PKI/TLS всё это отлично обеспечивает.

5.73 , нах , 19:23, 28/02/2018 [^] [ответить] [смотреть все] +1 + / – > Что не как не помешает тому CA что выдал ваш сертификат, распространять
> его побайтовые копии копии среди третьих лиц.

вы бы это... хоть википедию бы почитали, что-ли.

Побайтовая копия и так выдается каждому юзеру, посетившему твой сайт. Но вместе с ней выдается кое-что еще, и CA в этом никак не участвует.

> Само наличие CA, ака третьей стороны, которой все должны доверять по умолчанию,
> является профанацией понятия безопасность.

профанацией являются попытки делать выводы, не разбираясь в предмете.
CA не отвечает за безопасность твоего соединения. CA только подтверждает тот факт, что сертификат, предъявленный той стороной, подлинный, и выдан более-менее тому человеку, которому на момент выдачи принадлежал сайт. А не тов.майор посередке сам себе его выдал специально ради тебя.

2.71 , нах , 19:13, 28/02/2018 [^] [ответить] [смотреть все] [показать ветку] –1 + / –
> Т.е. конечного владельца сертификата это мало должно волновать?

да, он просто получит письмо щастья примерно такого содержания:
бла-бла-бла, despite our best efforts твой сертификат продлению не подлежит, а через пол-года и вовсе автоматически превратится в тыкву, вместе с CA его выдавшим, экипаж желает тебе приятного полета.

И идет подключать троянский скрипт для letsencrypt. Совершенно случайно именно в этот момент научившийся wildcard.

1.19 , Аноним , 11:14, 28/02/2018 [ответить] [смотреть все] –4 + / – Вроде только к сертификатам привыкли Буквально пару лет назад у юзверей-сайтошл...
весь текст скрыт
[
показать
]

2.36
Аноним
^
ответить
смотреть все
показать ветку
+
–
Все быстро, решительно сочуствуем туповатым юзверям-сайтошлепам.

2.37 , Аноним , 13:05, 28/02/2018 [^] [ответить] [смотреть все] [показать ветку] +2 + / –
Расслабься, больно не будет. Даже ничего не почувствуешь.
1.22 , поледанныхотсутств , 11:18, 28/02/2018 [ответить] [смотреть все] +5 + / –
Даёшь все сертификаты в публичный децентрализованный блокчейн!
2.30 , Аноним , 12:44, 28/02/2018 [^] [ответить смотреть все показать ветку + –
Намного лучшее решение, чем просто дать левым Васям полное право удостоверять... показать ветку
4.59 , Kuromi , 16:35, 28/02/201 ^ ответить смотреть все + –
"Отличная шутка" (c) Петросян

4.69 , Stop , 19:00, 28/02/2018 [^] [ответить] [смотреть все] + / – Первый раз вижу Мишу без минусов.
1.23 , Аноним , 12:16, 28/02/2018 [ответить] [смотреть все] –1 + / – Когда уже эту сертификацию сделают простой до немогу
2.31 , Аноним , 12:45, 28/02/2018 [^] [ответить смотреть все показать ветку + –
3.39 , Аноним , 13:07, 28/02/2018 [^] [ответить смотреть все + –
Неужто в федорке до сих пор нет letsencrypt, а не certbot ... показать]
4.41 , Аноним , 13:14, 28/02/2018 [^] [ответить

Автор:
27.02.18 22:57 -

смотреть все
+
–
code dnf provides letsencrypt-certbot-0.21 1-1 fc27 noarch code ... показать]
весь текст скрыт [

1.25 , Аноним , 12:37, 28/02/2018 [ответить] [смотреть все] + / – кстати блокчейн это похоже как раз для этого отлично подойдет, а вот для денег о...
весь текст скрыт
[
показать
]

1.35
,
X4asd
, 12:50, 28/02/2018 [
ответить
] [
смотреть все
]
+
/
–
а потом когда логирующих серверов тоже образуется челая куча -- они придумают ещё один серер с цифровой подписью который будет проверять что логирующие серверы тоже не накосячили?

то есть -- не проще ли тогда было бы -- наоборот -- удалить все CA-центры кроме например одного.

вместо придумывания очередной контролирующей сущности?

2.40 , Аноним , 13:10, 28/02/2018 [^] [
ответить
смотреть все
показать ветку
+
–

2.43 , Аноним , 13:21, 28/02/2018 [^] [ответить] [смотреть все] [показать ветку] +2 +
/
–

ЦА не нужны Нужно как в ssh, если что-то поменялось при подключении сразу сообщ...
весь текст скрыт
[
показать
] [
показать ветку
]
2.72
,
нах
, 19:15, 28/02/2018 [
^
] [
ответить
] [
смотреть все
] [
показать ветку
]
+
/
–
> то есть -- не проще ли тогда было бы -- наоборот --
> удалить все CA-центры кроме например одного.

принадлежащего гуглю. Именно над этим и работаем.

> вместо придумывания очередной контролирующей сущности?

это временная подпорка.

1.44 , Аноним , 13:22, 28/02/2018 [ответить] [смотреть все] + / – Очередной велосипед по захвату власти над сертификатами Как по мне возможность ...
весь текст скрыт
[
показать
]

1.46
,
никто
, 13:42, 28/02/2018 [

Автор:
27.02.18 22:57 -

ответить
] [
смотреть все
]
–2
+
/
–
слудующий шаг отказ от CA :-)

Когда каждый сможет туда запихнуть свой самоподписанный церт и тем самым поддтвердить что верить ему можно.

1.48 , хрю , 14:28, 28/02/2018 [ответить] [смотреть все] + / – Усё пытаются и пытаются плохую концепция са подпорками подпереть.
ню-ню - бох в помощь.

2.65 , Crazy Alex , 17:20, 28/02/2018 [^] [
ответить
смотреть все
показать ветку
+
–
Частенько в итоге получаются вполне рабочие штуки. TCP/IP тот же вспомнить - там костылей -

3.83 , Майнер , 07:10, 01/03/2018 [^] [
ответить
смотреть все
к модератору
+
–
Просто роутеры не умеют в SCTP...

1.75 , Аноним , 21:33, 28/02/2018 [ответить] [смотреть все] [к модератору] +1 + /
–
И это правильно Надеюсь можно будет внести УЦ в исключения ...
весь текст скрыт
[
показать
]

1.82
,
Аноним

, 01:41, 01/03/2018 [
ответить
] [
смотреть все
] [
к модератору
]
+
/
–
Мы конечно рады за компнию Гугль, что они в своём собственнном ЦА выписали себе ...
весь текст скрыт
[
показать
]

Read more http://www.opennet.ru/opennews/art.shtml?num=48159