一、差分隐私（Differential Privacy)与隐私保护

（一）相关论文

1、AI 时代隐私保护---Apple 案例：http://www.leiphone.com/news/201606/dtUSybvNaHTNZl0J.html

2、山东大学硕士论文：隐私保护的位置统计数据发布研究

3、The Algorithmic Foundations of Differential Privacy

（二）基本概念：

差分隐私，简单讲，就是向包含个人信息的数据中注入大量噪音，在隐私保护和数据分析之间取得平衡，确保每个人的个人信息不会被泄露。

（三）笔记：

差分隐私目前还在研究阶段，大型商用的可能性也未能得到确定。但在密码学据说有重要的地位和发展前景，或许能在深度学习和大数据时代成为隐私保护的潮流。但我们在使用的时候还要思考怎么在数据分析的基础上做到定向分析，差分隐私实质上是模糊了用户的身份使其难以被作为个体识别，这和我们进行个人征信管理好像有所出入。能不能假设一种算法的存在在数据中加入噪音，使未经审核或没有交易需求的第三方在从区块链获取信息的时候，得到的数据没法与具体的个体相对应，而在双方有信用评估需求的时候可以通过公钥私钥之类的进行个体的定位。

二、利用区块链（公钥/私钥）进行公开隐私保护

以下是知乎关于医疗机构利用区块链保护用户隐私的案例，可以看一下：

https://www.zhihu.com/question/40475025/answer/86750297

MIT Media LAB：关于数字证书与隐私的两篇文章。MIT 试图在区块链上构建证书，利用公钥/私钥使用法来认证使用者和接受者，内容经过加密，而且可以进行撤销。

‘Certificates, Reputation, and the Blockchain ’ （链接需翻墙）
https://medium.com/mit-media-lab/certificates-reputation-and-the-blockchain-aee03622426f#.aad4p03s5

‘What we learned from designing an academic certificates system on the blockchain’
https://medium.com/mit-media-lab/what-we-learned-from-designing-an-academic-certificates-system-on-the-blockchain-34ba5874f196#.wljhp83mr

What is it？

The trail of credentials and achievements that we generate throughout our lives says something about who we are, and it can open doors that allow us to become who we want to be. Some credentials, such as university degrees, are more important than others. But at the end of the day, all of these credentials represent experiences that are part of our lives.

How it Works？

Issuing a certificate is relatively simple: we create a digital file that contains some basic information such as the name of the recipient, the name of the issuer (MIT Media Lab), an issue date, etc. We then sign the contents of the certificate using a private key to which only the Media Lab has access, and append that signature to the certificate itself. Next we create a hash, which is a short string that can be used to verify that nobody has tampered with the content of the certificate. And finally we use our private key again to create a record on the Bitcoin blockchain that states we issued a certain certificate to a certain person on a certain date. Our system makes it possible to verify who a certificate was issued to, by whom, and validate the content of the certificate itself.

Framework

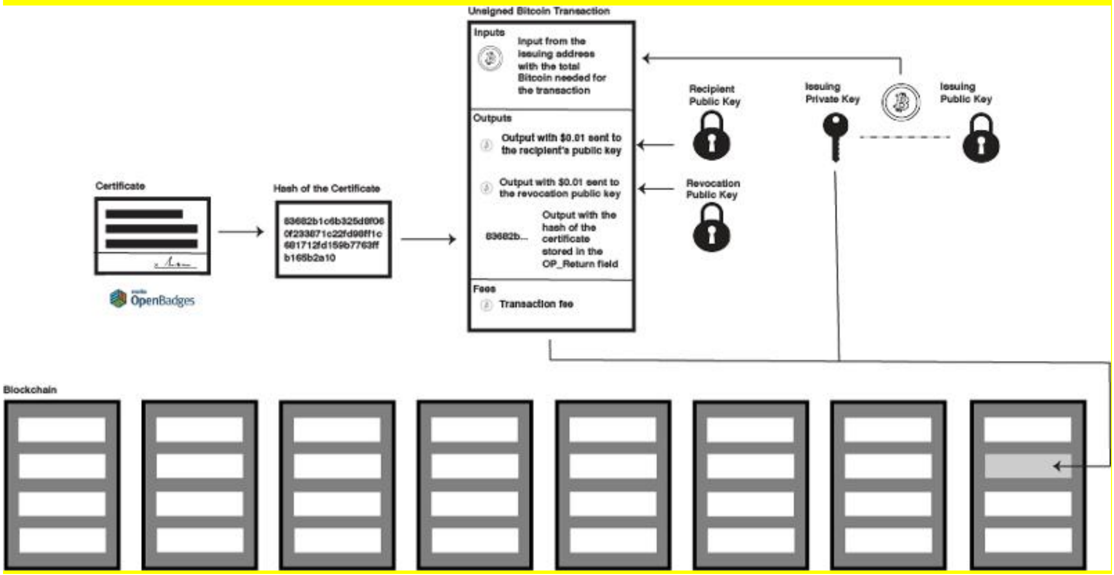
Cert-schema describes the data standard for digital certificates. A digital certificate is essentially a JSON file with the necessary fields needed for our cert-issuer code to place it on the blockchain. We tried to keep the schema as close to the open badges specification as possible and expect to be even more closely aligned with the next version of the specification.

Cert-issuer takes a JSON certificate, creates a hash (a short string that can be used to uniquely identify a larger digital file) of the certificate, and issues a certificate by broadcasting a Bitcoin transaction from the issuing institution's address to a recipient's address with the hash embedded within the OP_RETURN field.

Cert-viewer is used to display and verify digital certificates after they have been issued. The viewer code also provides the ability for users to request certificates and to generate a new Bitcoin identity.

Public/private Keys

Our system uses public/private key pairs to authenticate an issuer as well as a recipient. While that's a powerful concept, we found it was a bit of a headache to implement in practice. Ideally certificate recipients (such as graduates or workshop participants) would create their own key-pairs and then share their public key with us in order to request a certificate. But the amount of technical sophistication required to do this makes a broad roll-out prohibitive. For now, the ability to share a simple link to a certificate is convenient, but in the future, we will need better ways for non-technical users to create and manage their own keys. The best solution would be a wallet for academic credentials that works like the wallets used to hold and transact Bitcoin. An alternative would be to use a paper-based system of pre-creating and sharing keys (and then destroying them). But that requires a higher level of trust in the institution that issues the certificates.


Unsigned Bitcoin Transaction
Inputs
Input from the issuing address with the total Bitcoin needed for the transaction
Outputs
Output with $0.01 sent to the recipient's public key
Output with $0.01 sent to the revocation public key
83682b...
Output with the hash of the certificate stored in the OP_Return field
Fees
Transaction fee
Recipient Public Key
Issuing Private Key
Issuing Public Key
Revocation Public Key
Certificate
OpenBadges
Hash of the Certificate
83682b1c6b325d8f06
0f233871c22fd98ff1c
681712fd159b7763ff
b165b2a10
Blockchain

Privacy

While much has been made of the ability to conduct shady business on the blockchain, it is inherently a public and immutable space–everyone has access to its contents and nothing can be erased. At the same time, certificates are only useful when they can be tied to a person. That's why protecting private data is so important. On one hand, learners need to be able to show evidence that they (and not somebody else) received a particular certificate. At the same time, they should be able to disclose this information to one employer, without having to also share it with every other employer.

三、零知识证明（ZKPs）进行隐私保护

原文网址：
http://www.coindesk.com/trend-towards-blockchain-privacy-zero-knowledge-proofs/
译文网址：
http://news.blockchain.hk/trend-towards-blockchain-privacy-zero-knowledge-proofs/

基本概念：零知识证明是指允许双方（证明者和验证者）来证明某个提议是真实的，而无须泄露除了它是真实的之外的任何信息。

摘要：当你创建隐私和私密性解决方案时需要有很多折中权衡。最主要的是会牺牲透明度，而这也是第一个区块链比特币区块链所最主要的特征。按照最初的设计，区块链是一个透明的机器。在这个系统中，计算机是分布式的，没有一个实体能够控制网络。不仅仅如此，任何人都可以是验证者，而且任何人都可以书写或读取网络上的数据。客户端和验证者可以是匿名的，每一个节点都在本地存储所有的数据。这使得所有交易数据都是公开的。

比特币的安全是通过一个验证过程来实现的，其中所有的参与者都各独立并自发地验证交易。比特币是通过使用匿名的地址来解决隐私问题的，但仍然可以通过各种技术来找到谁在使用该地址。

这在私有区块链领域是截然相反的，在私有区块链中，去中心化和透明度并不是必要的。

重要的是隐私和私密性、速度和可扩展性（随着更多的节点加入区块链，能够维持很高的速度表现）。加密的点对点交易意味着只有这两个参与交易的人才能接收到数据。在很多系统中，可以有第三方节点（监管者）加入来成为交易的一部分。

Zcash 操作实例：（from Zcash Whitepaper）

Value in Zcash is ***carried by notes****, which specify an amount and a paying key. T****he paying key is part of a payment address, which is a destination to which notes can be sent****. As in Bitcoin, this is associated with a private key that can be used to spend notes sent to the address; in Zcash this is called a spending key.*

A payment address includes ***two public keys****: a paying key matching that of notes sent to the address, and a transmission key for a key-private asymmetric encryption scheme. "Key-private" means that ciphertexts do not reveal information about which key they were encrypted to, except to a holder of the corresponding private key, which in this context is called the viewing key. This facility is used to communicate encrypted output notes on the block chain to their intended recipient, who can use the viewing key to scan the block chain for notes addressed to them and then decrypt those notes.*

The basis of the privacy properties of Zcash is that when a note is spent, the spender only proves that some commitment for it had been revealed, without revealing which one. This implies that a spent note cannot be linked to the transaction in which it was created."

四、通过比特币私密交易探讨隐私保护

侧链进行私密交易：http://www.8btc.com/confidential
原文：https://people.xiph.org/~greg/confidential_values.txt

比特币使用地址部分解决隐私问题，如果人们不知道哪个用户拥有某些地址，隐私能得到保证。但是只要你和其他人交易，你就知道了对方至少一个地址。从这个地址开始，你可以追踪到其他相关联地址，并且评估交易金额和留存金额。举例说：假定你的老板用比特币支付你工资，你后来用这些比特币来支付你的房租和食品。你的房东和超市都知道了你的收入，当你的收入提高时，他们有可能提高给你的价格，或者把你当成盗窃的目标。

目前已经有些技术来进一步提升比特币隐私性（如 CoinJoin，以联合支付方式来合并交易），但是这些技术的应用不多，因为有可能追踪到金额。

还有另外一些在竞争链中提出的密码学技术来提升隐私，但是他们都破坏了“剪枝”（比特币创世文章第 7 部分），使得用户需要一个永远增长的数据库来验证新交易，因为这些系统

不知道币是否已经被花费。大多数密码学隐私系统的性能较差，高负载或需要很强密码学假设（而且不易懂）。

私密交易使得交易金额更隐私，同时能让公众网络来验证留存的区块链交易，做到这些无需在比特币系统中新增新的密码学假设，并且系统开销可控。

由于加法同态承诺的密码学技术，CT（私密交易）是可行的，另一方面，CT 还启用了附加的隐私“备忘”数据（如发票号或撤款地址）交换，且通过回收大多数 CT 密码学证明的开销，使得交易大小不会增加。