14th Annual Triangle InfoSeCon Conference
*Raleigh Convention Center, Friday, October 26, 2018*
Track 6, Room 303, 10:15 – 11:05 AM

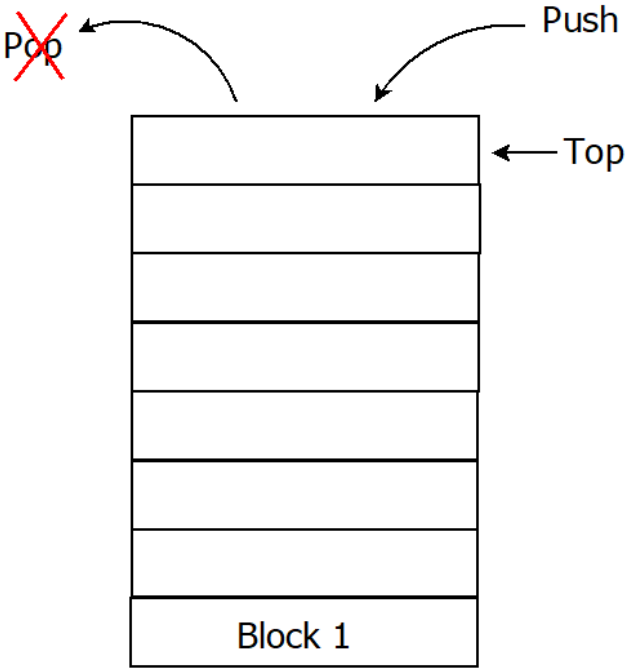
# Privacy Preserving Blockchains

**Phillip H. Griffin**

*Griffin Information Security*

# What is a blockchain?

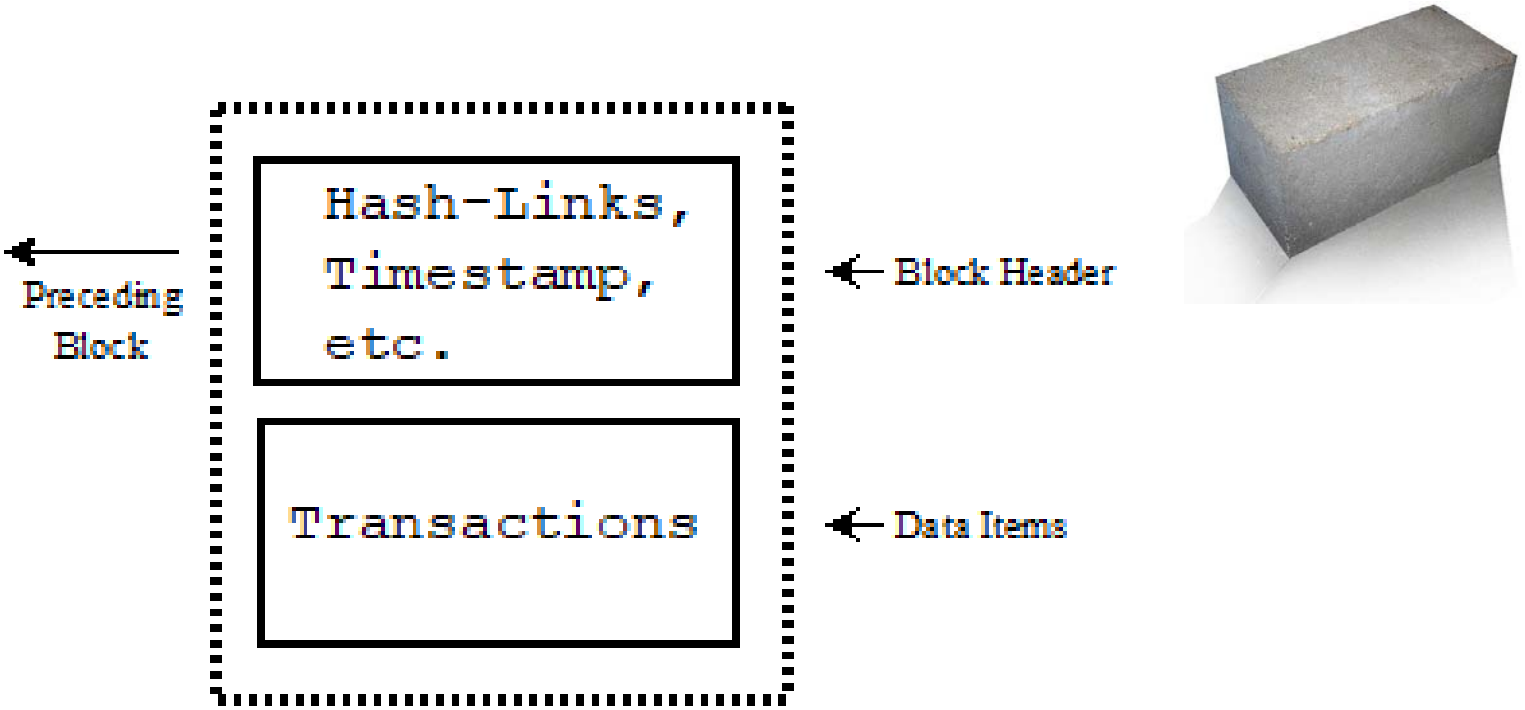
A signed series of hash-linked, append only, time stamped data sets.




As a data structure, a blockchain can be viewed as a '**stack**' with limited operations.

# What is a block?

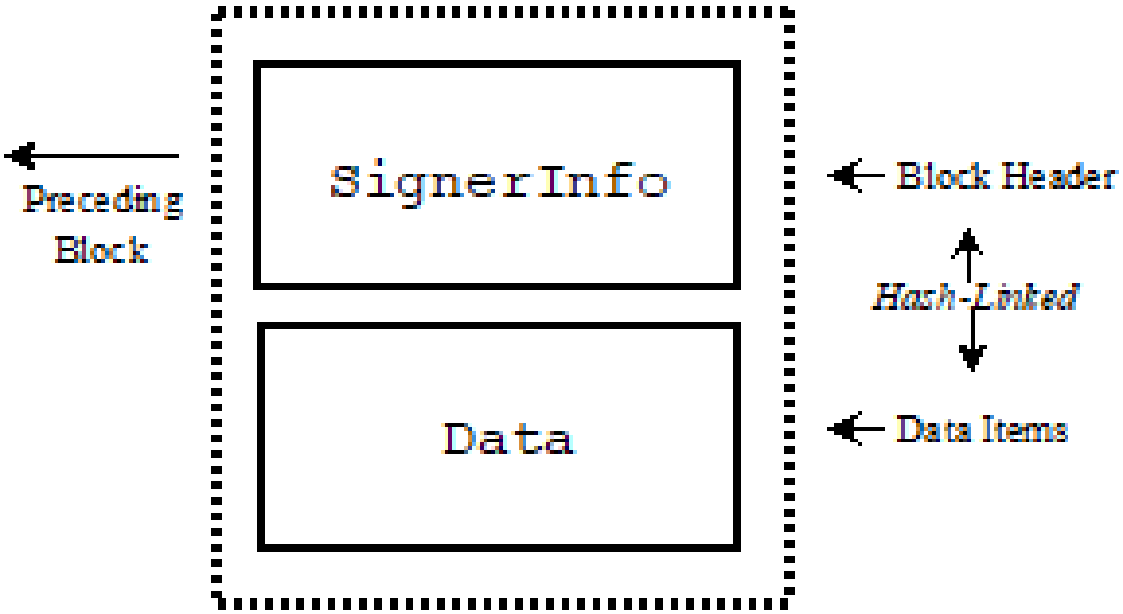
A blockchain block is composed of a ***block header*** and a set of ***data items***.




The data items may be referred to as a collection of transactions. The block header contains a hash of the data items and a hash that links the prior block to this block.

# SignedData block

A signed series of hash-linked, append only, time stamped sets of data items.




As a data structure, a blockchain can be viewed as a '**stack**' with limited operations.

# Schema Benefits

**Widely Deployed Mature Protocol:**

- RSA Public Key Cryptography Standards (PKCS) #7 - CMS
- IETF S/MIME CMS Standards – Secure Electronic Mail
- X9.73 CMS for use in the Financial Services
- X.894 Cryptographic Message Syntax (CMS)

**Abstract Syntax Notation One (ASN.1) Schema Definition Language**

- Defines X.509 Certificates and Directory Access Protocol (DAP)
- Used in Information Exchange Protocols: 3GPP, RFID, UMTS, etc.
- Cryptographic Algorithm and Key Management – ECDSA, EdDSA, RSA

**Automated Programming Language Code Generation**

- Schema-Based Code For Application Programming Interface (API)
- Java, C, C++ Programming Languages For Hundreds of Platforms

# SignedData Attributes

**What types of attributes can be included in a block header ?**

- Message Digest — *Hash of the block data being signed*
- Content Type — *Type of the block data being signed*

- Time Stamp — *Date and time that the block data is signed*
- Previous Block — ***Hash-Pointer** of the previous block's signed attributes*

- Sidechain Block — ***Hash-Pointer** to block or external information object*
- Data Location — *Location of the data being signed (May be detached)*
- Tokenization Manifest — *Off-chain cryptographic data protection*

# Extended Hash-Pointer

**A pointer to an object, the object's hash , and its data type**

```
HashPointer ::= SEQUENCE {
   hash         DigestedData  OPTIONAL,
   pointers     Pointers  OPTIONAL
} (ALL EXCEPT ({ -- None present -- }))

Pointers ::=  SEQUENCE SIZE(1..MAX) OF pointer Pointer

Pointer ::= CHOICE {
   uri        URI,
   rfid       RFID,
   gps        GPS,
   address    Address,
   dbRecord   DBRecord,

   ...   -- Expect other pointer types --
}
```

# Tokenization Manifest

**Provides data confidentiality and preserves privacy of sensitive user data**

- Tokenization can be encryption based or rely on other techniques
- Can store **{Token, Hash( Data ), URI, }** in a block with Data protected off line
- URI can point to a Tokenization Service Provider (TSP) who controls access
- Off-line data deleted on user demand does not affect blockchain integrity
- Any type or data format can be tokenized; tokenization can be field level
- Participant membership can be restricted on a per-sidechain basis

# Off-Chain Tokenization

**Fields of data in any format can be redacted by defining a manifest**

A redaction manifest for XML markup can be a series of XPath expressions.

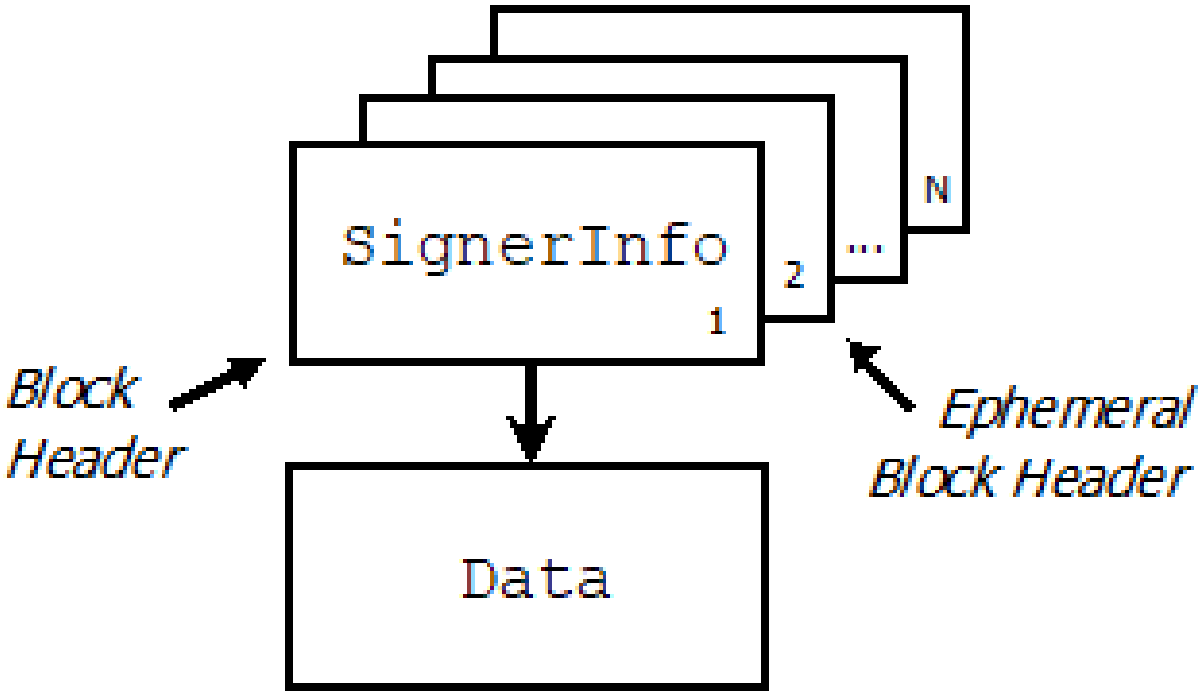
```
<xPathSet>
   <xpath> /A/Second/C </xpath>
   <xpath> /A/Second/C/Fourth[2]/Fifth  </xpath>
</xPathSet>
```

A redaction manifest for an image can be represented as a series of pairs of {x, y} coordinates that define the corners of a rectangular area in the image.

```
<image>
   <rectangle>  23,  48,  42, 82 </ rectangle>
   <rectangle> 433, 112, 670, 234 </ rectangle>
</ image>
```

# SignerInfos

SignedData permits multiple signers, each signer with their own signature algorithm, key, and any number of signed attributes of any type or format




SignerInfos is a set of values of type SignerInfo , which can serve as a block header

Each SignerInfo instance in the set can be used to create one Ephemeral Sidechain

# Ephemeral Sidechains

**Can be added to, or deleted from any block at any time**


- Makes ***right-to-be-forgotten*** blockchain data privacy possible
- Unlimited number of ephemeral sidechains for any block
- Each sidechain can reside in a different geographic location
- Sidechains are policy, algorithm, and consensus protocol independent
- Efficient resource-constrained environment storage management
- Participant membership can be restricted on a per-sidechain basis

# Deeper Dive

[1] S. Nakamoto, "Bitcoin: A Peer-To-Peer Electronic Cash System," 2008.

[2] Griffin, P. (2018). An Internet of Block Things. ITU Journal – ICT Discoveries, No. 2 – Data for Good. Retrieved September 30, 2018, from phillipgriffin.com/whitepapers/

[3] Griffin, P. (2018Privacy Preserving Blockchains. China Communications: Blockchain Technology and Applications. Vol. 15, No. 12. Retrieved September 30, 2018, from phillipgriffin.com/whitepapers/

[4] X9.73:2017 *Cryptographic Message Syntax (CMS) – ASN.1 and XML.* American National Standards Institute (ANSI).

[5] Griffin, P. and Stapleton, J. "Data element tokenization management". United States Patent 10,025,941, July 17, 2018.

[6] ITU-T Recommendation X.894 Generic applications of ASN.1 – Cryptographic Message Syntax (CMS), October 13, 2018.

# Questions?

phil@phillipgriffin.com +1 (919) 622 -7049