洋蔥好吃嗎

更深的網路

I. 表網 (Surface Web，又稱「表層網絡」或「開放網絡」)

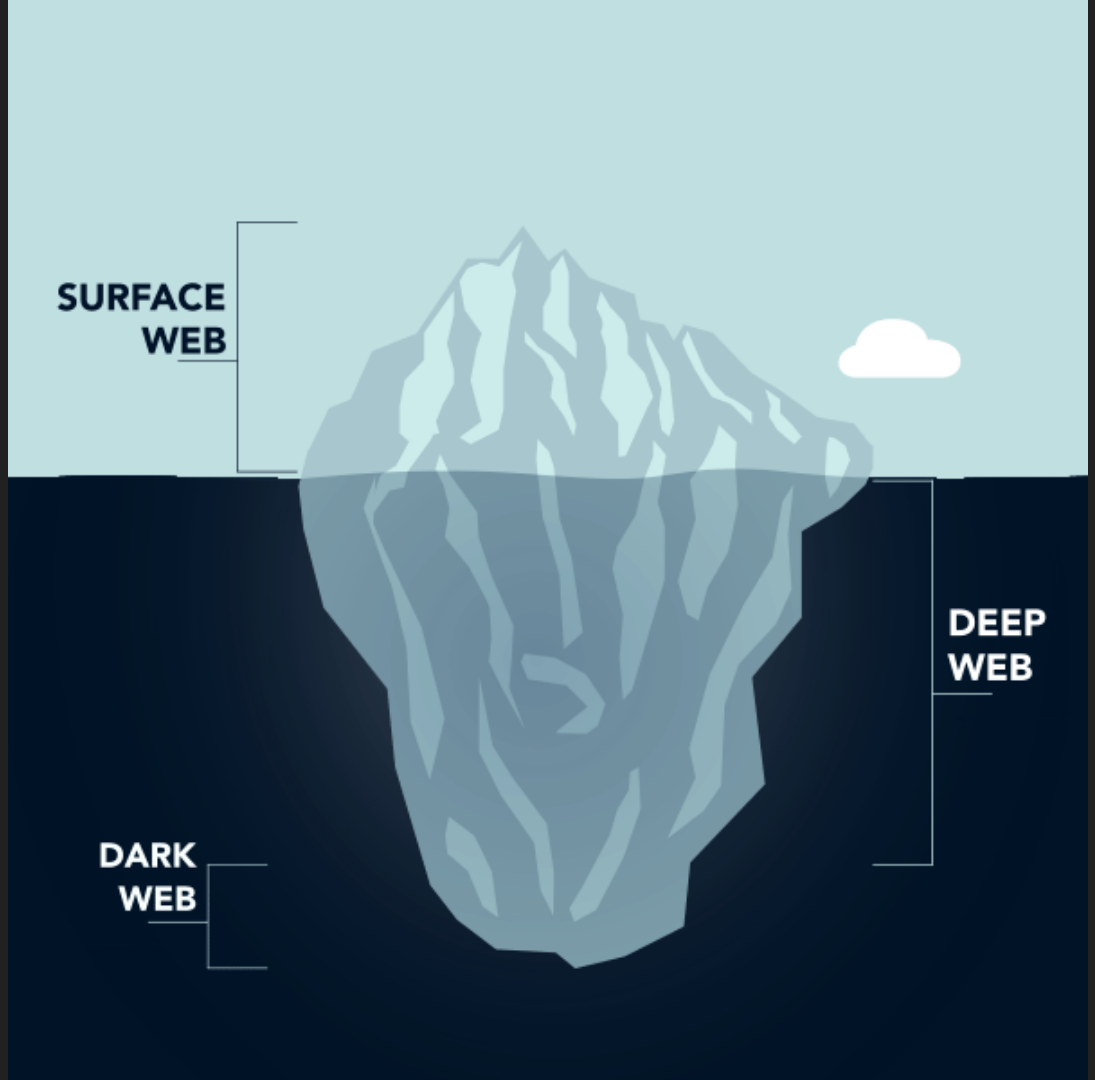
表網是大眾日常會到訪的網站和平台，如新聞媒體、網上商店、社交平台等。用戶使用一般搜尋器(例如Google、Yahoo等)便能找到有關連結。表網的數據佔互聯網的資訊大約4%。

II. 深網 (Deep Web)

深網的內容不能被一般搜尋器找到，例如公司內聯網、即時通訊軟件的對話等，它佔整個互聯網的資訊大約90%。深網的資訊大多需要密碼或身分驗證後才能接觸到，例如醫療報告、政府內部文件、公司商業資料、以及必須付費才能使用的服務，如線上雜誌和報紙等。

III. 暗網 (Dark Web 或 Dark Net)

暗網的內容只能透過特殊軟體、授權或通訊標準存取。暗網社群以洋蔥網絡 (The Onion Router，俗稱Tor) 最為活耀，其次是隱形網計劃(Invisible Internet Project (I2P))和自由網(Freenet)，暗網的設計讓用戶身分高度隱密，暗網社群之間也不能互通，它佔整個互聯網的資訊大約6%。現時，不法分子利用暗網的隱密性和匿名性作犯罪活動，如販賣毒品、槍械、兒童色情物品、販賣信用卡資料和個人資料等。

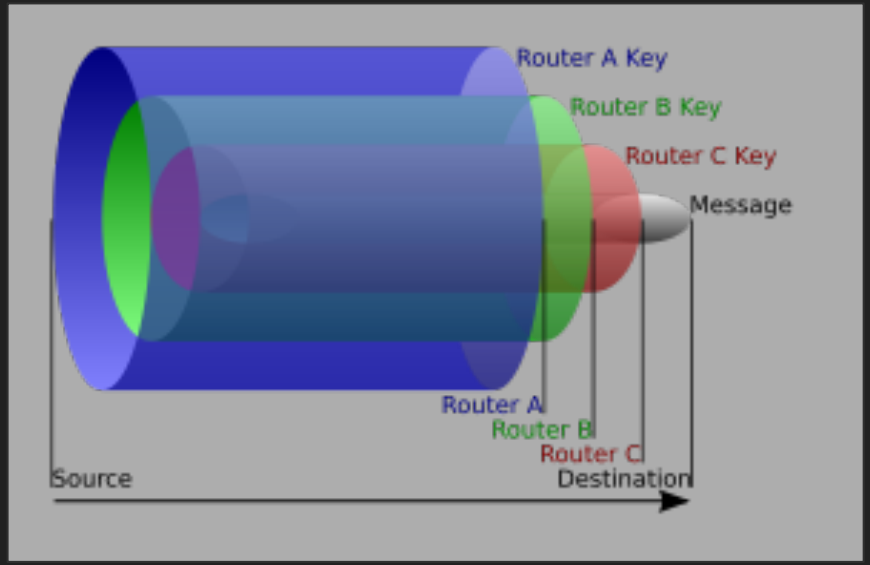

SURFACE
WEB
DEEP
WEB
DARK
WEB

吃顆洋蔥

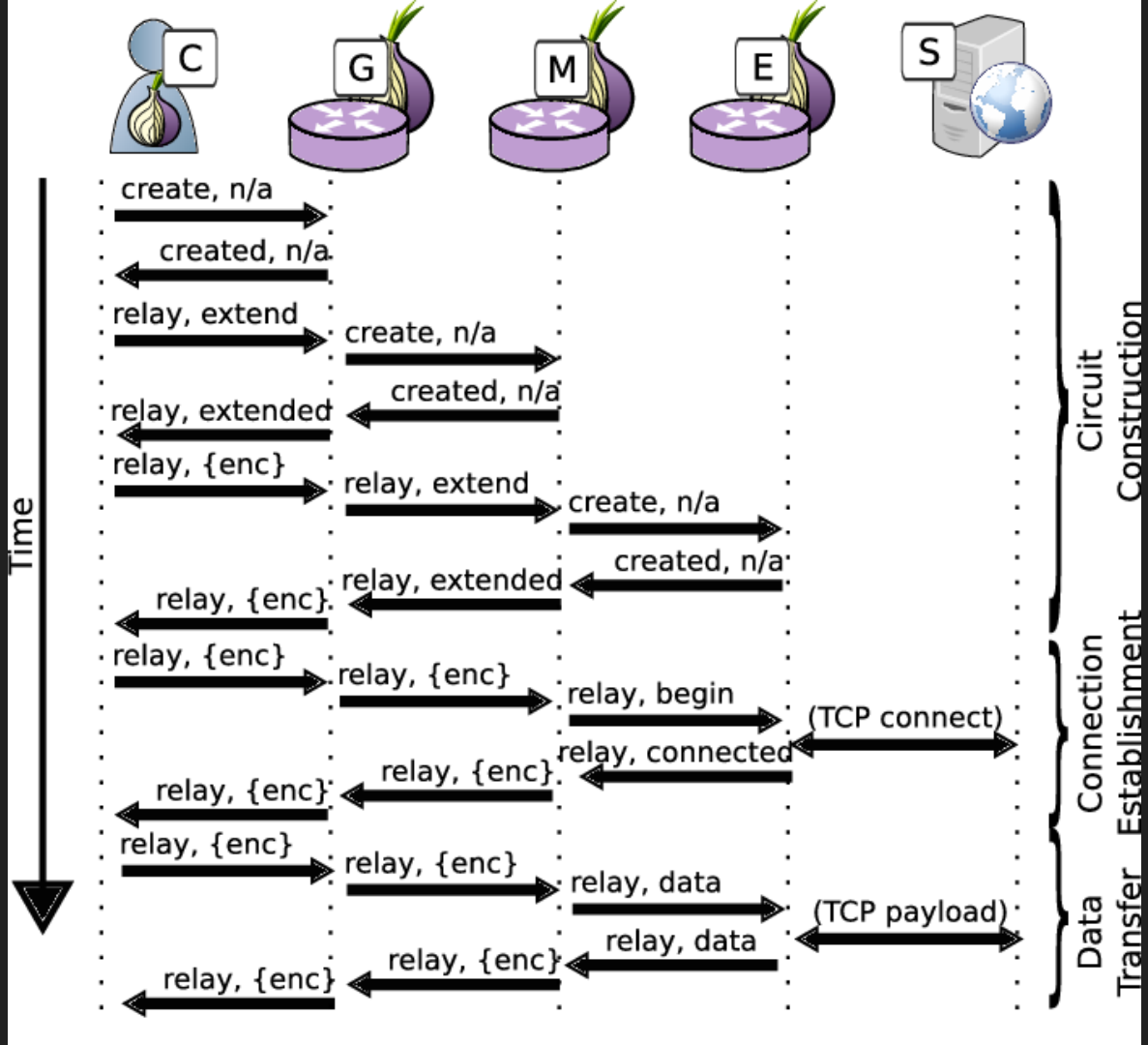
於1990年代中期，美國海軍研究實驗室的人員認為當時的互聯網通訊不夠保密，擔心黑客的截取通訊活動會影響軍事安全，因而開發洋蔥網絡 (Tor)。Tor的原理是把訊息作多層加密，在通過每一個多個節點(node)時才進行一層解密，多層加密訊息的結構猶如洋蔥形狀。Tor網站使用.onion作為頂層網域名(有別於一般使用的 .com、.hk、.org等)，用戶需要透過特定的軟件訪問特殊的節點，才能瀏覽Tor網站。

Tor 的基本思路是：利用多個節點轉送封包，並且透過密碼學保證每個節點僅有局部資訊，沒有全局資訊，例如：每個節點皆無法同時得知請求端與響應端的 IP，也無法解析線路的完整組成。

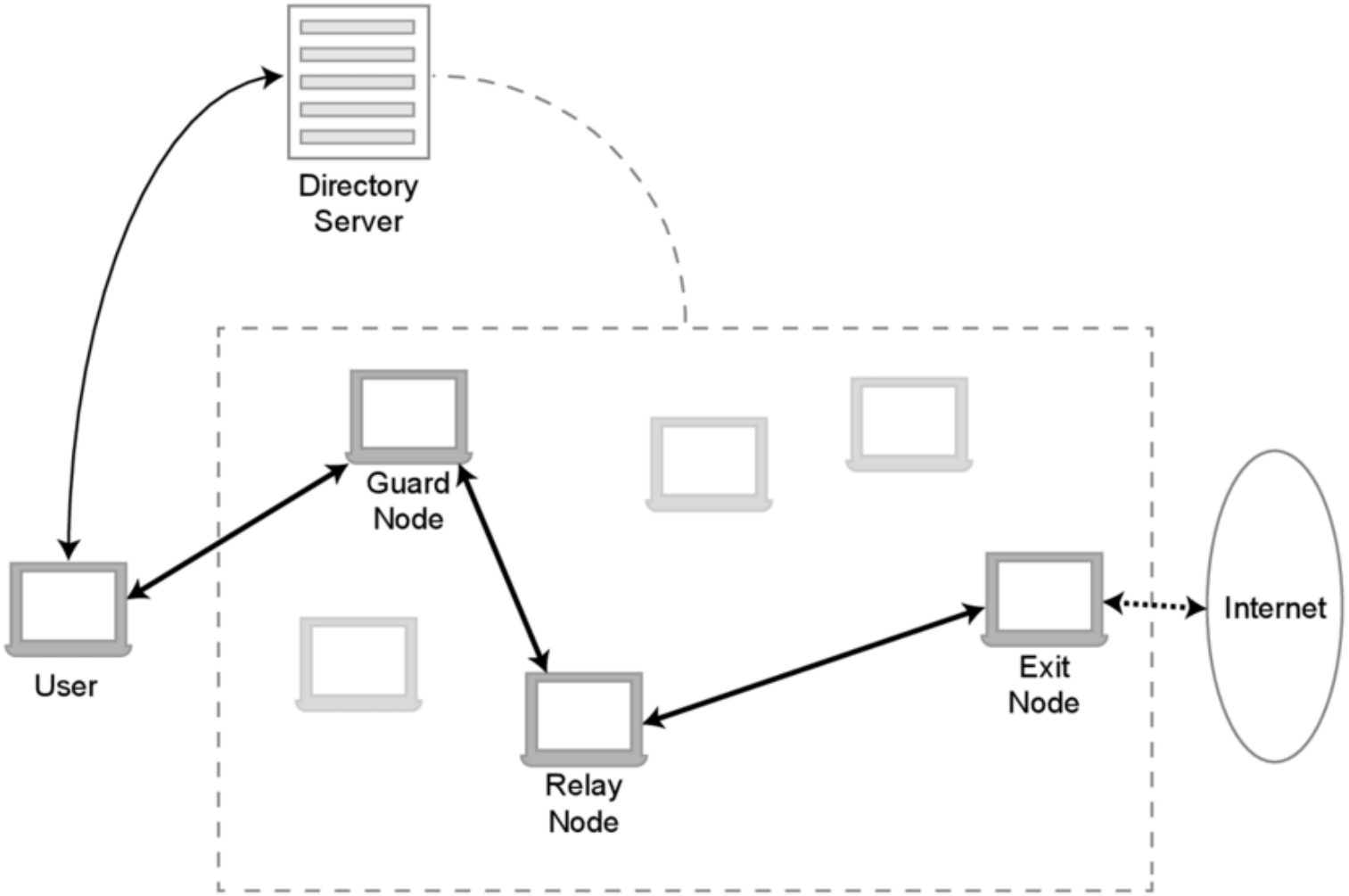
被稱作洋蔥路由的原因在於訊息一層一層的加密包裝成被稱作洋蔥封包的資料結構，層數取決於到目的地中間會經過的節點數，每經過一個節點層會將封包的最外層解密，因此任一個節點都無法同時知曉這個訊息最初與最終的目的地，使發送者達到匿名的效果。



發送者首先將封包傳送給路由器A，解密了藍色一層，並發現要傳給B，而封包傳送至B時又解密了綠色一層，同理再傳給C，而C在解密了紅色一層後得到原始要傳送的訊息並將之傳給目的地。


C
G
M
E
S
Time
create, n/a
created, n/a
relay, extend
create, n/a
created, n/a
relay, extended
relay, {enc}
relay, extend
create, n/a
created, n/a
relay, extended
relay, {enc}
relay, {enc}
relay, {enc}
relay, begin
(TCP connect)
relay, connected
relay, {enc}
relay, {enc}
relay, {enc}
relay, {enc}
relay, data
(TCP payload)
relay, data
relay, {enc}
relay, {enc}
Circuit Construction
Connection Establishment
Data Transfer

Tor 引入了目錄伺服器（Directory Server）此一設計。目錄伺服器會列出 Tor 網路中所有可用的節點，請求端可以透過目錄伺服器選擇可用的洋蔥路由器以建立線路。目前 Tor 網路中有 9 個分別由不同組織維護的目錄，中心化的程度相當高，這也成為 Tor 安全上的隱憂。

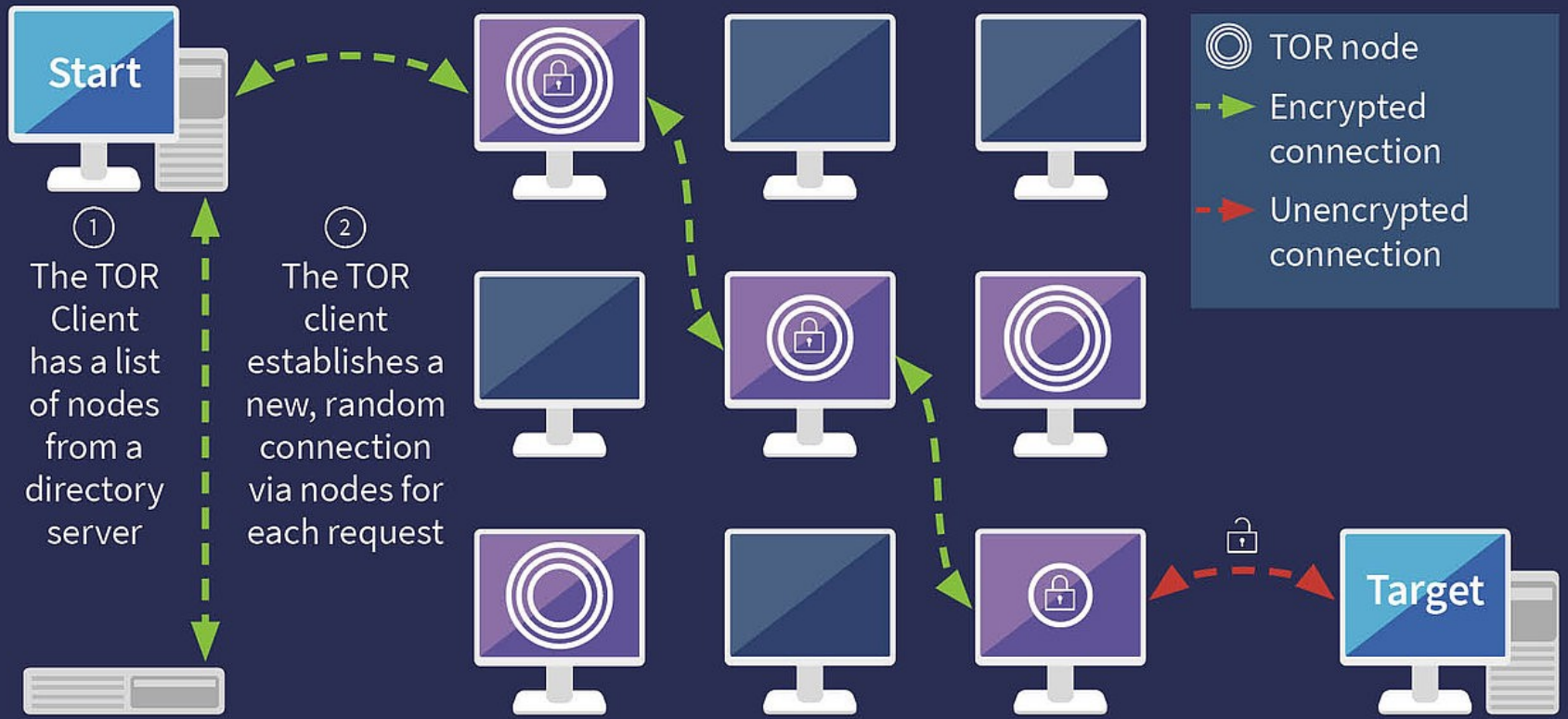

Directory
Server
Guard
Node
User
Relay
Node
Exit
Node
Internet

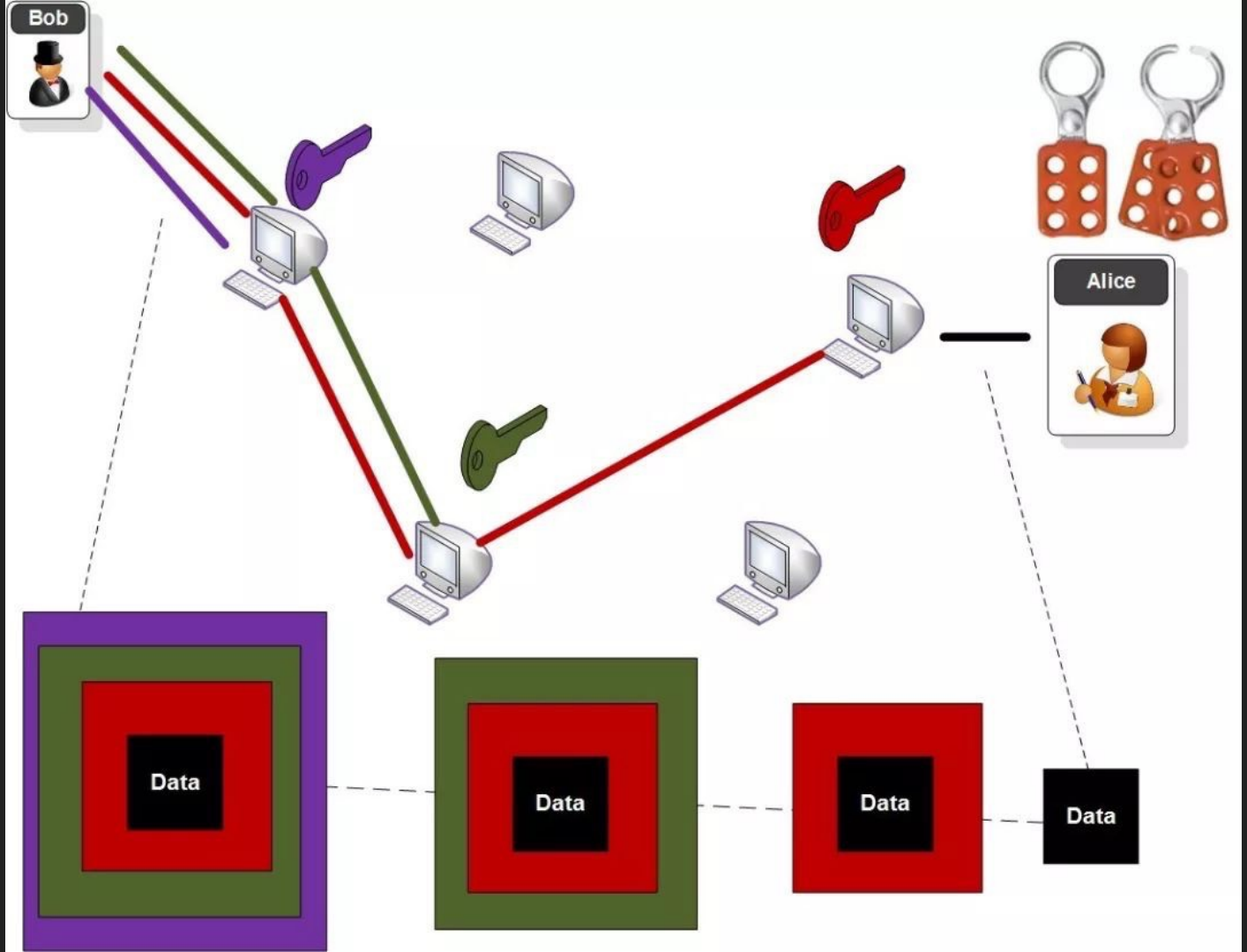
為了傳送洋蔥封包，發送訊息者會從「目錄節點」（directory node）提供的列表中選取一些節點，並以這些規劃出一條被稱作「鏈」（chain）或「線路」（circuit）的傳送路徑，這條路徑將為傳輸封包所用。為了確保發送者的匿名性，任一節點都無法知道在鏈中自己的前一個節點是發送者還是鏈上的另一節點；同理，任一節點也無法知道在鏈中自己的下一節點是目的地還是鏈上另一節點。只有鏈上的最後一個節點知道自己是鏈上最終節點，該節點被稱作「出口節點」（exit node）。

洋蔥路由網路使用非對稱加密，發送者從目錄節點獲得一把公開金鑰，用之將要傳送的訊息加密並傳送給鏈上的第一個節點，該節點又被稱作入口節點（entry node）；其後與之建立連線和共享密鑰。建立連線後發送者就可以通過這條連線傳送加密過的訊息至鏈上的第二個節點，該訊息將只有第二個節點可以解密；當第二個節點收到此訊息後，便會與前一個節點也就是入口節點同樣的建立連線，使發送者的加密連線延伸到它，但第二個節點並不曉得前一個節點在鏈中的身分。之後按照同樣原理，發送者通過入口節點和第二個節點的這條加密連線將只有第三個節點能解密的訊息傳送給第三個節點，第三節點同樣的與第二個節點建立連線；藉由重複相同的步驟，發送者能產生一條越來越長的連線，但在效能上仍有限制。

當鏈上的連線都建立後，發送者就可以透過其傳送資料並保持匿名性。當目的地回送資料時，鏈上的節點會透過同一條連線將資料回傳，且一樣對資料層層加密，但加密的順序與發送者完全相反；原發送者收到目的地回傳的資料時，將僅剩最內一層加密，此時對其解密就可拿到目的地回送的訊息。

How does the **TOR** network work?




Bob
Alice
Data
Data
Data
Data

洋蔥V2

.onion頂級域的位址為Tor服務組態完成後，由公鑰自動生成的難以記憶且不便理解的十六位半字母半數字hash。這種十六位的hash由字母表內任意字母與2至7的十進位數字所組成，以此來表示使用base32加密後的80位元數字。通過平行計算生成大量的金鑰對的方式來尋找合適的URL並設立起人類可讀的.onion位址是可行的（例如以組織名開頭）。

ou37jngrs7lolacxttyacn6fdepcthdoseajo27liefu5fzqldl2zqid.onion

洋蔥V3

v2 與 v3 最大的差異就是本來 v2 的 hostname 是 16 個英數字 (大約是 80-bit security)，現在 v3 變成是 56 個英數字 (大約是 280-bit security)，大幅降低 collision 的機會。

1. September 15th, 2020

0.4.4.x: Tor will start warning onion service operators and clients that v2 is deprecated and will be obsolete in version 0.4.6.

2. July 15th, 2021

0.4.6.x: Tor will no longer support v2 and support will be removed from the code base.

3. October 15th, 2021

We will release new Tor client stable versions for all supported series that will disable v2.

V2 and V3

V2

- 已不再是預設版本
- Shorter names that are a hash of the RSA public key of the onion service
- Malicious HSDirs can snoop on and determine the address of v2 onion services for which they are serving descriptors (and will get removed from the network if they get caught doing it)
- 較差的加密
- 程式碼難以理解

V3

- 目前預設版本
- Longer names that encode the actual ed25519 key of the onion service into the name
- Malicious HSDirs cannot snoop. No one will ever find out your onion service exists unless you tell them
- 較好的加密
- 更乾淨的程式碼

自己種洋蔥

sudo apt install tor

sudo vim /etc/tor/torrc 取消註解

HiddenServiceDir /var/lib/tor/hidden_service/

HiddenServicePort 80 127.0.0.1:80

sudo service tor stop

sudo service tor start

sudo cat /var/lib/tor/hidden_service/hostname

sudo apt install nginx

sudo service nginx start

sudo vim /etc/nginx/nginx.conf 取消註解

```
service_tokens off;
port_in_redirect off;
service_name_in_redirect off;
```

sudo service nginx restart

Tor Browser 11.5現可自動偵測並繞過國家審查

有些國家為了審查境內用戶，封鎖了Tor網路的存取，例如中國、俄羅斯、白俄羅斯或土庫曼等，使得Tor Browser用戶必須手動變更Tor的網路設定，找出可繞過封鎖的途徑，不過，Tor Browser 11.5所內建的Connection Assist 1.0版，將可自動偵測及繞過各國的封鎖。

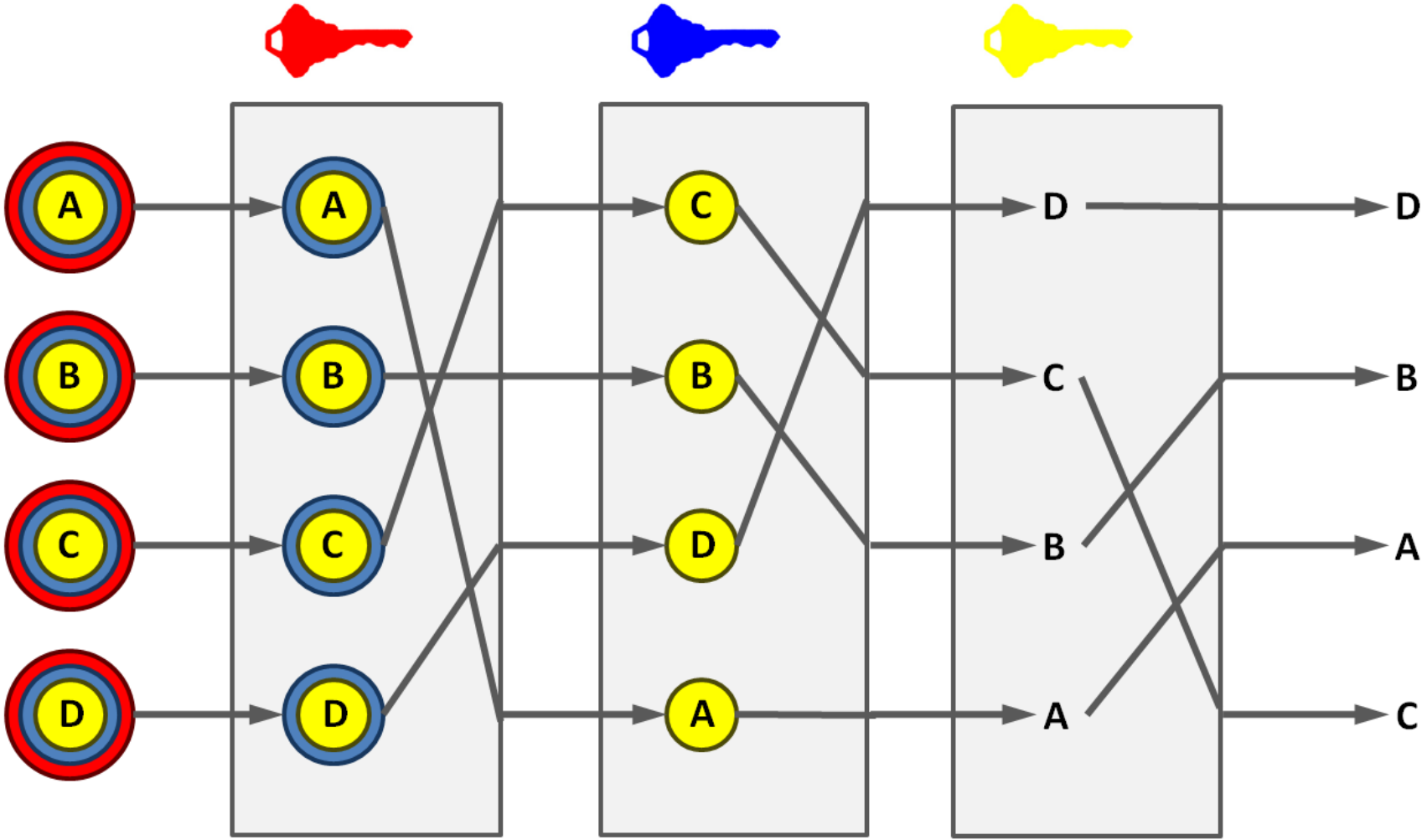
Connection Assist可查找及下載每個國家可繞過封鎖之各種選項的最新列表，並自動部署最適合使用者區域的設定，使用者還可儲存這些用來連結Tor網路的橋接資訊，並透過複製或QR code分享，例如分享給Android版的Tor Browser。

吃點其他的

混合網路（Mix Network）早在 1981 年就由 David Chaum 發明出來了，可以說是匿名技術的始祖。

洋蔥路由的安全性奠基於「攻擊者無法獲得全局資訊」的假設，然而一旦有攻擊者具有監控多個 ISP 流量的能力，則攻擊者仍然可以獲知線路的組成，並對其進行流量分析；混合網路則不僅會混合線路節點，還會混合來自不同節點的訊息，就算攻擊者可以監控全球 ISP 的流量，混合網路也能保證維持匿名性。

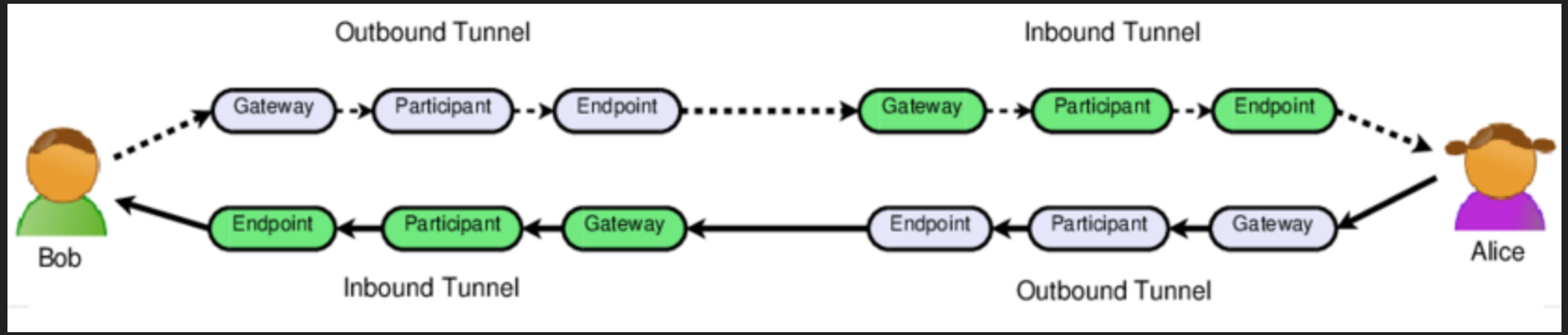
然而高安全性的代價就是高延遲（Latency），這導致混合網路無法被大規模應用，或許洋蔥路由的設計是一種為了實現低延遲的妥協。


A
B
C
D
A
B
C
D
C
B
D
A
D
C
B
A
D
B
A
C

混合網路啟發了洋蔥路由，洋蔥路由也啟發了大蒜路由。2003年上線的 I2P（Invisible Internet Project）便是基於大蒜路由（Garlic Routing）的開源軟體，可以視為是去中心化版的 Tor。幾乎所有大蒜路由中的組件，在洋蔥路由中都有對應的概念：例如大蒜路由的隧道（Tunnel）即是洋蔥路由的線路；I2P 的網路資料庫（NetDB）即是 Tor 的目錄；I2P 中的匿名服務（Eepsite）即是 Tor 的洋蔥服務。

不過，大蒜路由也有其創新之處：它允許多個封包共用隧道以節省建立隧道的成本，且其使用的網路資料庫實際上是一個分散式雜湊表（DHT），這使 I2P 的運作徹底去中心化。

I2P 最大的詬病就是連線速度太慢，一個缺乏激勵的去中心化網路恐怕很難吸引足夠的節點願意持續貢獻頻寬與電費。


Outbound Tunnel
Inbound Tunnel
Gateway
Participant
Endpoint
Gateway
Participant
Endpoint
Bob
Alice
Endpoint
Participant
Gateway
Endpoint
Participant
Gateway
Inbound Tunnel
Outbound Tunnel

全新的專案

Dusk：實作大蒜路由的區塊鏈，不過官方已宣布因其影響網路效能而暫停開發此功能。

cMix：透過預先計算（Precomputation）以實現低延遲的混合網路，是混合網路發明者 David Chaum 近期的研究，值得期待。

Loki：結合 Monero 與 Tor/I2P 的區塊鏈 ，並使用代幣激勵節點貢獻頻寬與電力，由其白皮書可以看出發明者對於匿名技術的熱愛與信仰。

於主流區塊鏈的提案

比特幣：全世界第一條區塊鏈，將於其網路使用一個不同於洋蔥路由的匿名技術：Dandelion++，該匿名技術因其訊息傳播路徑的形狀類似浦公英而得其名。

閃電網路（Lightning Network）：知名的比特幣第二層方案，將於其網路內實作洋蔥路由。

Monero：使用環簽章保護用戶隱私的區塊鏈，將於其網路內實作大蒜路由，已開發出 Kovri 並成為 I2P 官方認可的客戶端之一。

Tor - 维基百科，自由的百科全书

暗網· 守網者

洋葱路由- 维基百科，自由的百科全书

The components of the Tor network. After downloading the node list from...

[原创]一篇文章读懂Tor原理

隱私議題專欄｜讀懂什麼是「洋蔥路由Onion Routing」？改進區塊鏈的匿名技術

Tor 是什麼？公認最安全的上網方式- Tor 在使用時有什麼注意事項

Tor Browser 11.5現可自動偵測並繞過國家審查

.onion - 維基百科，自由的百科全書