現代社會網路發達為了避免代議政治的缺點並鼓勵公民參與，多有所謂網路投票，但是網路投票目前仍有幾個問題使得網路投票不可行：

1. 灌票。如果投票不具名，投票人可以自己寫一個灌票程式。這就是為什麼在票選名山的時候，玉山可以輸給一座鳥山，只是因為某個電腦技術高超的投票人在這座鳥山求婚成功。
2. 就算投票人沒有人灌票，因為投票沒具名，所以執政單位還是可以灌票；如果開票結果有人懷疑要求重新驗票，也頂多只能發現有領票的投票人有 100 人但是有投票的人（包含投廢票）卻有 110 人，無法得知哪 10 張票是不應記入投票結果。或者，執政單位可以偷偷把合法投票人的票塗鴉改成廢票，這 100 張票裡原本是選 A 有 60 張，選 B 有 35 張，廢票有 5 張，但是卻被執政單位改成，選 A 有 30 張，選 B 有 35 張，廢票有 35 張，此時即使有人懷疑展開重新驗票，也只能無語問蒼天，因為沒有人知道這張廢票是真廢票還是假廢票。
3. 賄選。因為上述理由，投票不能完全不具名。但是，如果投票具名，執政單位或任何人都可以賄選任何投票人。
4. 加害。因為具名，執政單位可以限制特定投票人無法跑票，否則會扁他，所以即使某個屬於此執政黨的人正義感突然發作想跑票，也會因為擔心被加害而不敢跑票。

怎麼辦呢？請繼續往下看。

所以我們只好放棄絕對結果的投票，改採接受些許錯誤的投票結果。意思是，例如被投票的選項有 A 和 B，真正的結果應該是 A 當選，但是開票的結果可能 1000 次選舉裡面有一次會說 B 當選。這樣的誤差在實際上是可以接受的，因為沒有規定說投票人要終身不改其志（我大學時候一位同學是藍，去留學後變為綠），所以隔一個月之後同樣議題的真實投票結果可能又是另外一個結果；既然上帝給的 free-will 導致的結果不同都可以接受了，這種統計錯誤應該也無傷大雅了。

如果接受這種觀點。請繼續往下看。

操作的方式是這樣，A123456789 代表任一投票人：

Step 1　想要投票的人拿著自己的 privatekey（自然人憑證裡面有一個）去 sign 一個訊息"我 A123456789 要投票"，然後把這個電子訊息公開。因為 privatekey 只有自己有，所以任何人都可以藉由 A123456789 的 publickey 去確認 A123456789 真的要投票。因為訊息是公開，行政單位也沒辦法一手遮天說 A123456789 其實沒有想投票。

Step 2　如果想投廢票，那 A123456789 就不用做下述動作。

Step 3　A123456789 躲到任何隱密的地方，拿出十元硬幣投兩次，來決定被問的問題，投十元硬幣有兩個可能：

case I　　如果都沒有人頭。被問的問題是："你是要選 A 嗎？"。

case II　　其他情形。被問的問題是："你是要選 B 嗎？"。

Step 4　如果答案是 yes，就用自己的 privatekey 去 sign 一個訊息"Y"，如果答案是 no，就用自己的 privatekey 去 sign 一個訊息"N"，然後把這個電子訊息公開。

因為訊息都公開，所以沒有人能阻擋訊息的揭露，任何人都可以當計票員，沒有人可以隻手遮天投票結果（畢竟執政單位的計票也許不可信），這無法灌票，因為 A123456789 的選票只有一張。計票員首先用

A123456789 的 publickey 去確認 A123456789 的 Y 或 N 的訊息屬實未經竄改，但是問題有 1/4 的機率是"你是要選 A 嗎？"，有 3/4 的機率卻是"你是要選 B 嗎？"。如果我想賄賂，因為我要行賄 A123456789 的先決條件是要知道 A123456789 真正投票時候丟的兩個銅板的結果，但是即使 A123456789 把他的丟銅板的動作和 sign 答案的動作和公開的動作拍下來寄給我，我還是會高度懷疑 A123456789 只是詐騙集團，想騙取我的行賄金，那個影片只是拍給我看的，畢竟沒有一個 " official " 投票機或投票所會出現在影片裡讓我確認那個影片是 A123456789 真正投票時候發生的事。如果我想加害，因為 A123456789 不會把他丟銅板的結果揭漏給我，所以我無從知道他是選 A 還是 B。因為資訊是權力的來源而沒有任何人有能力知道 A123456789 的選擇，所以沒有任何人可以賄賂或加害 A123456789。

Step 5　收集結果。總共有有效票 n 張，答 Y 的有 f 張。以 x 代表開票結果選 A 的投票人的比例，因為 Pr[Y]=Pr[case I] Pr[Y | case I]+ Pr[case II] Pr[Y | case II]，所以 f/n =1/4*x + 3/4*(1-x)，所以開票結果選 A 的投票人的比例是 3/2− 2f/n

交出 privatekey 的動作可以拿錢也可以不拿錢，有拿錢稱之為 " 補償金 "（因為要承受必然之惡，就像如果南田部落同意核電的廢料儲存，可以拿到的錢，用來 compensate 未來可能的醫療支出），不再叫做 " 行賄金 "，因為都已經攤在陽光下不再是罪惡；很慷慨沒有拿錢的稱之為 " 任命代理人 "。因為所有的事都內部化（internalized），所以外部性（Coase externalities）的消費者剩餘損失就消失了。

其實整個系統最重要的是自己決定要選 A 還是 B。因為自己決定要選 A 還是 B 是個可能很花計算資源的工作。如果不知道自己想選 A 或 B，那就如同把自己投票的這個 privatekey 交給所選的立法委員，然後所有代議政治的問題就都跑出來了，也沒有人能幫自己辯白真正的選擇。所以整個系統其實應該要加個 Step0："少看點督教授，把時間拿來傷腦筋"。如果你真的不想花腦筋，需要個代理人，那就 sign 個訊息 " 我把 privatekey 交給 / 賣給 B123456789 "（全世界都知道你交出去 privatekey 了），這個人就是你的立法委員，承認這些必然之惡，也拿了 compensate，也不要動不動就占據街頭說立法委員是豬了。

---

何謂 privatekey 或 publickey？

一個盒子，有兩個鑰匙孔，分別有兩把鑰匙，一個在左一個在右，這個盒子如果用左（右）邊鑰匙去鎖就只能用右（左）邊鑰匙去開。左鑰匙就是 privatekey，右鑰匙就是 piblickey。privatekey 全世界只有我有，publickey 每個人都可以輕易公開取得。所以如果有人要寫一個 for-my-eye-only 的訊息，只要把訊息用我的 publickey 鎖起來傳給我就可以。如果我要寫一個訊息讓別人相信真的是我寫的，我只要把這個訊息用我的 privatekey 鎖起來傳給別人。如果蘇菲瑪索要寫個秘密的 for-my-eye-only 的訊息給我，她只要把這個訊息用她的 privatekey 鎖起來緊接著用我的 publickey 鎖起來，然後傳給我，我收到後用我的 privatekey 打開緊接著用她的 publickey 打開，如果過程沒有問題，這個訊息就一定，不是冒充的蘇菲瑪索發出的給我的秘密訊息，也不可能有不是我的人可以讀。

何謂電子簽名 sign？

如果有一個函數，y=f(x)，計算很容易很快，但是反過來，已知 y 要去造一個 x，是天荒地老困難的問題，那這個函數就可以當作電子簽名的基礎，稱為 checksum。假設有一份我寫的文件，寫好後 e 給對方，我想讓對方確認這個傳遞處理過程中文件未經竄改，我只要把我的文件當作 x，丟到這個函數裡算出 checksum 是 y，然後能夠把 y 安全的拿給對方，對方收到文件後，計算文件的 checksum 得到 z，如果 y 和 z 一樣，那就是文件未經竄

改，否則就是有被竄改。接下來的問題是，我要如何把 y 安全的傳給對方呢？依據上述 privatekey/publickey 的知識，我把 y 用我的 privatekey 和對方的 publickey 鎖起來，傳給對方，就做完了。