數位貨幣與主權個人網路

加密與個人信任網路帶來資訊與價值自由

加州州立大學長堤分校 劉穎教授

大綱

問題與解決方案

方案的技術與理論基礎

思考維度

二種基本人權

世界（Universal）人權宣言第12條和美國憲法第四修正案表達的人類文明共識

- 資訊自由
  - 個人主權
  - 隱私
  - 自由交流
- 價值自由
  - 個人主權
  - 隱私控制
  - 自由交換

個人權益的現實困境

個人身份：依附機構（政府/商業公司）

資訊/價值的主權：機構有決定權

通訊與交易的審查、監控：個人失去使用權與隱私

通脹與鑄幣稅：政府操縱價值單位與價值分配

困境背後的原因

表徵

- 個人不擁有數字身份
- 被動信任政府與商業公司
- 無法控制信息交流與價值流動

根本

- 沒有屬於個人的數字資產來處理、存儲、傳輸信息
- 缺乏應對攻擊的防禦工具

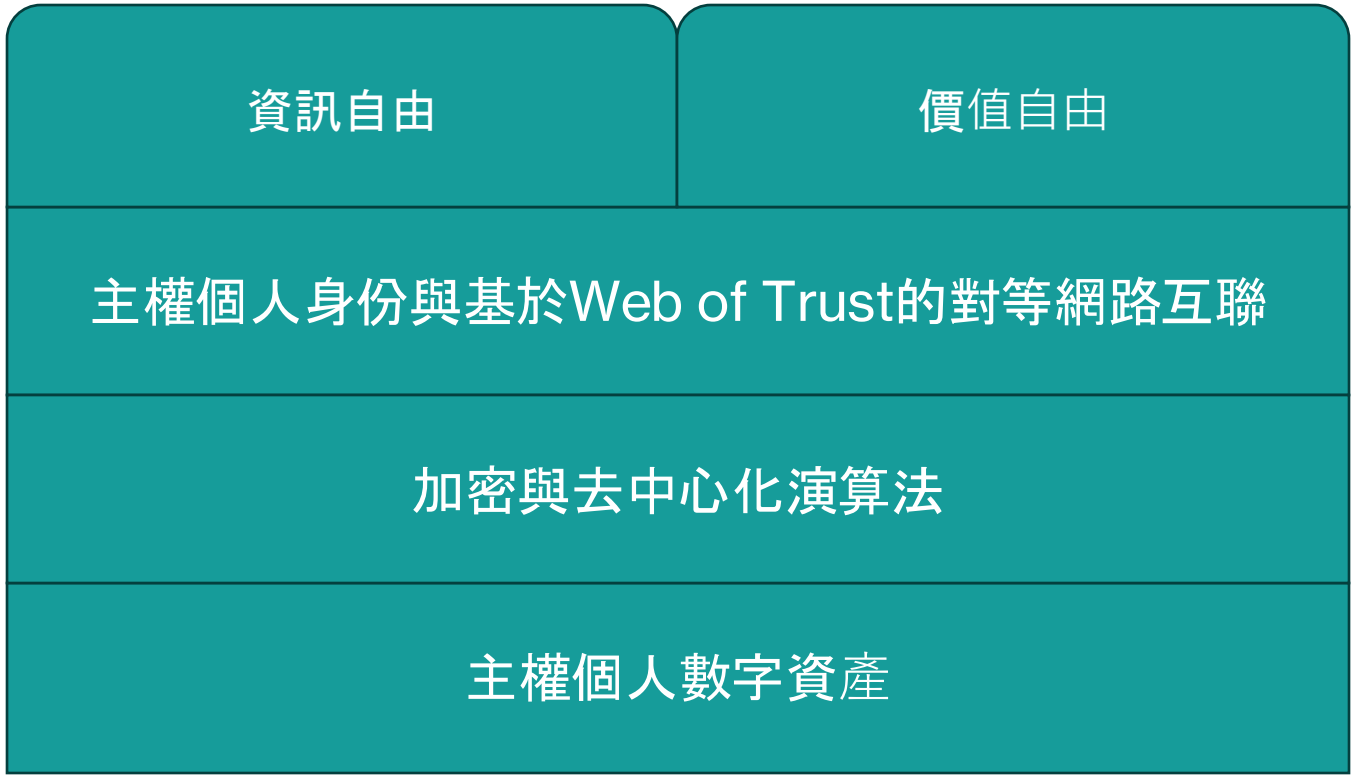
人權困境的解決方案

沒有個人數字身份 =》 主權個人數字身份

被動信任 =》 個人信任網（Web of Trust）

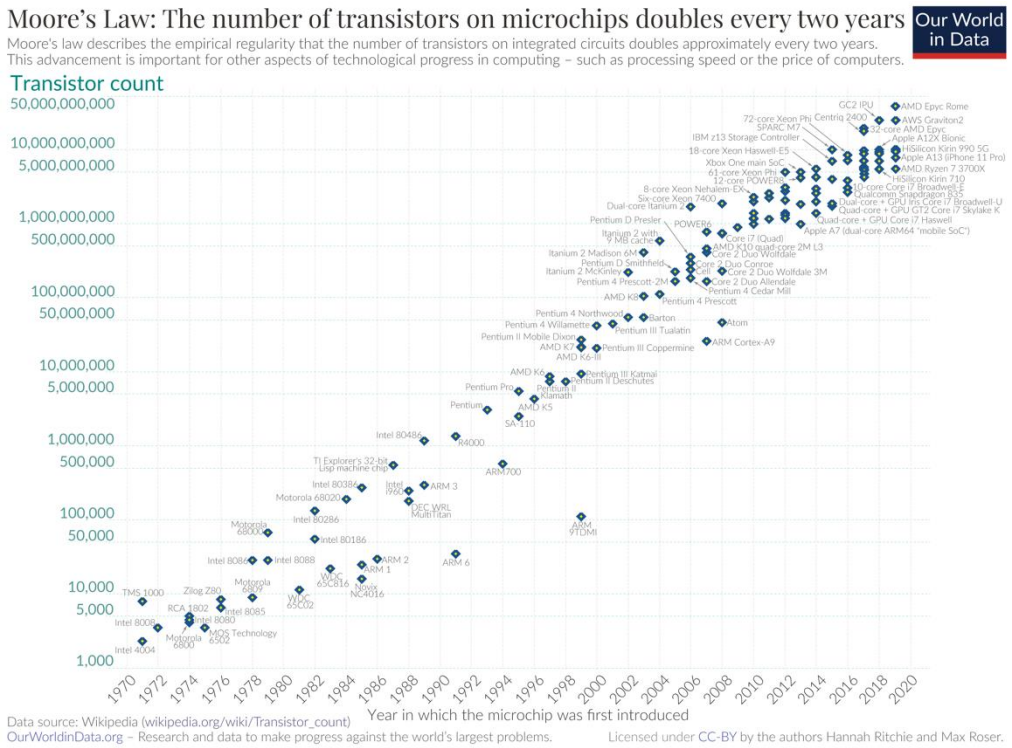
無法控制信息交流與價值流動 =》 加密技術與新通訊協議

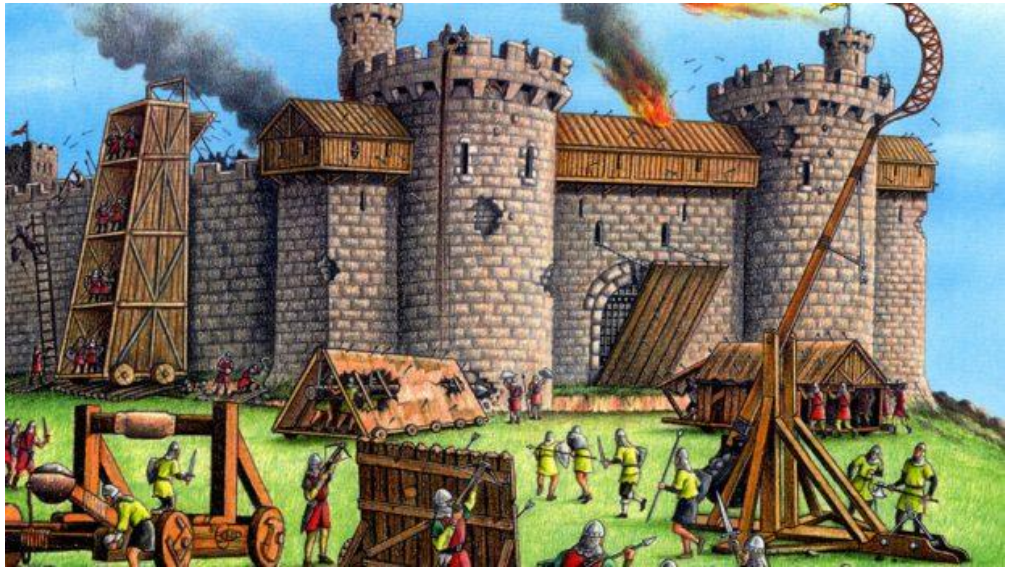
主權個人數字資產與加密防禦：從根本上解決問題



個人數位資產的技術基礎：
關於處理器、存儲器和通訊的摩爾定律

- 技術進步與開源
  - 2025年的 iPhone17 （about 35TFlops） 計算能力約等於1995年全世界的計算能力總和。
  - 開源軟體與硬體：低成本的知識共享与組合应用。
- 結果
  - $20/月主權私有雲計算可以支援普通人的計算需求





加密具有不對稱的防御能力

只需手拋256次硬幣產生的密鑰就可以抵禦國家級別的攻擊

- 個人主權數字身份：公
- 信息主權：加密
- 價值主權：信息時代的貨幣本質是一個具有全體共識的公共帳本

密碼學的特殊價值：去中心化

Dan Boneh，斯坦福大學教授在其密碼學課程裡提到：“Any function you'd like to compute, that you can compute with a trusted authority, you can also do without a trusted authority”.

source: https://www.coursera.org/learn/crypto/lecture/ubmLN/what-is-cryptography

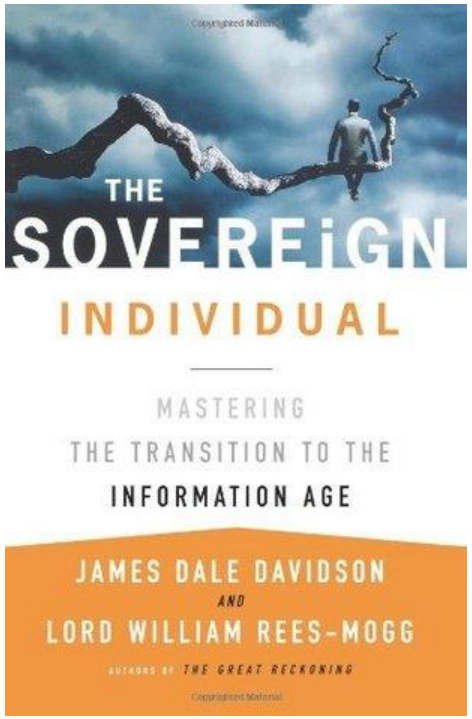
任何使用可信權威的函數計算，都可以在沒有可信權威的情況下完成。

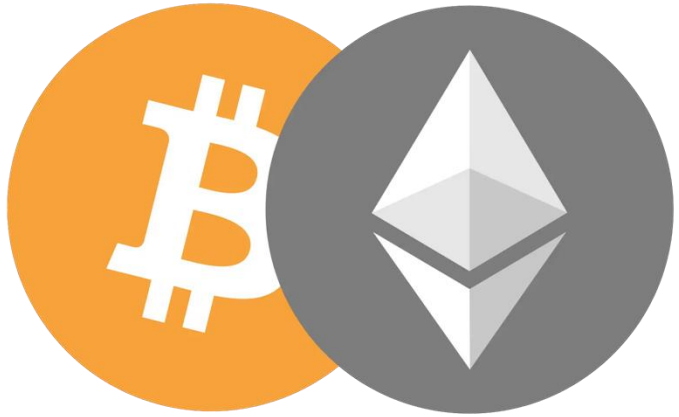
https://en.wikipedia.org/wiki/Dan_Boneh

所有的信息交流與價值交換都可以在沒有政府與公司的參與下完成。 比特幣的成功是一个具体證明。

主權個人（1997年出版）

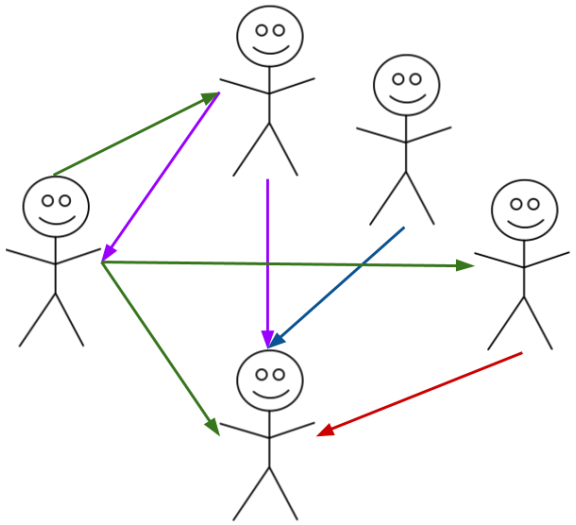
- 由於加密技術與互聯網，主權個人成為信息時代的基本組織架構，可以發揮人的最大潛力。
- “新技術使得財富擁有者拜託國家壟斷的控制...新世紀裏私有市場的互聯網錢幣會取代政府發行的法幣”
- Peter Thiel给新版作序：“加密貨幣是去中心化的，人工智慧是中心化的。或者，如果你想用更意識形態的表述，加密貨幣是个人自由主義的，而人工智慧是共產主義的。”

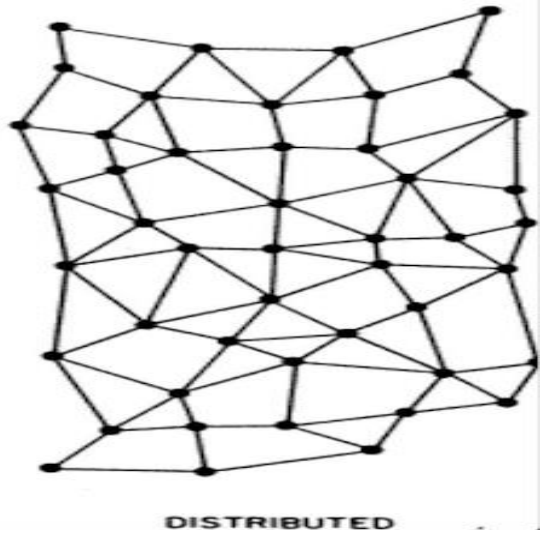




主權個人互聯網SovinWeb：Sovereign Individual Web

- 個人信任網路WoT （Web Of Trust）
  - 自己驗證和確定信任程度。
  - 利用現有信任系統：域名服務、銀行帳戶、身分證等。
- 所有WoT組成新的疊加在現有通信網路之上去中心化P2P對等網路SovinWeb。
  - 與基於全域共識區塊鏈的Web3不同，這是基於WoT的局部共識。





完整解決方案

資訊自由 創建、發佈、訂閱、社交	價值自由 比特幣、金融交易、社區經濟
主權個人身份與基於WoT的對等互聯網絡SovinWeb	
加密與去中心化演算法	
主權個人數字資產：後端的私有雲服務與前端智慧手機	

https://nektony.com/blog/how-to-use-icloud-storage-instead-of-phone-storage

二種資訊化模式

- 原子的製造使用， 資訊系統是輔助工具，也許重要但不是根本。
- 比特的製造使用，資訊是本質，資訊技術會顛覆行業。
  - 比如網飛Netflix顛覆百事達Blockbust
  - 股票交易員（右下圖是空蕩蕩的瑞銀交易大廳）被電腦取代。
  - 比特幣成為二萬億市值貨幣。

法幣和傳統銀行為什麼還沒有被顛覆？

理由

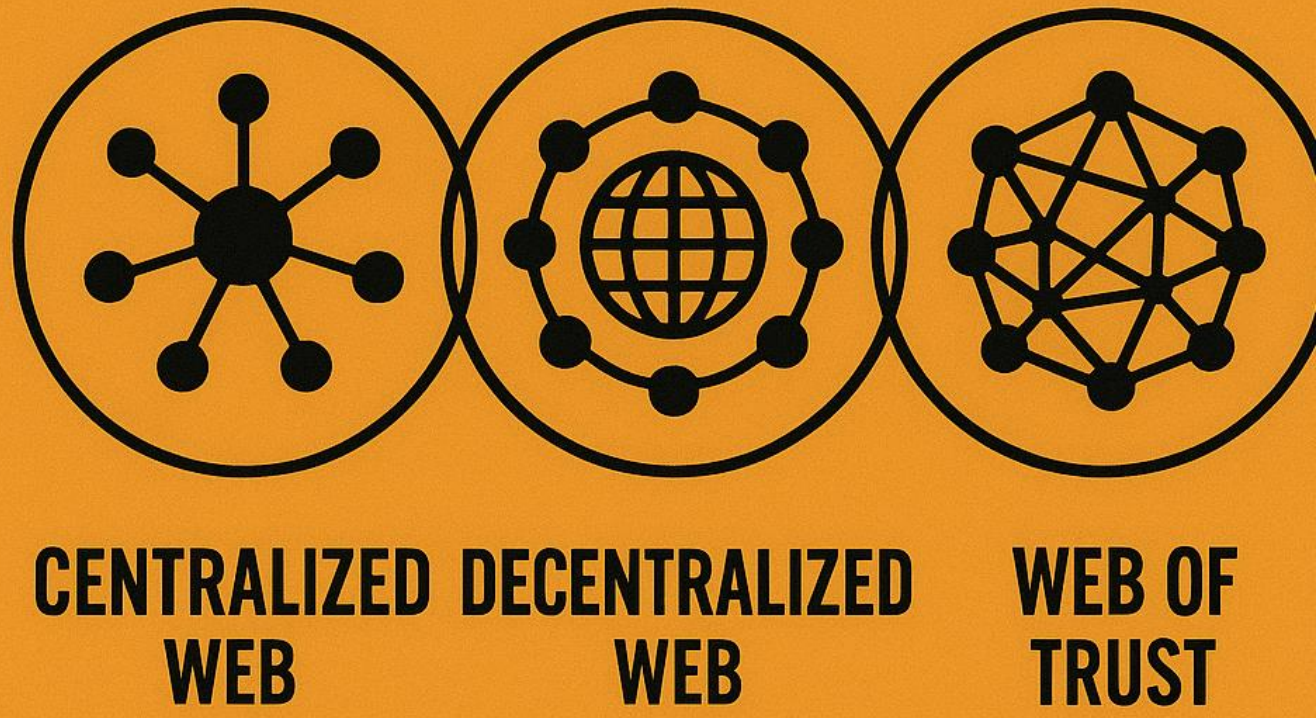
- 政府的控制與監管在很長一段時間仍處於支配地位。
- Z时代（1997-2012）之前出生的人對貨幣與金融的共識仍習慣於传统系統。

趨勢

- 主權個人會掌控信息交流與價值交換。
- Z世代之後多數人作為数字原生代的共識改變。

三種信任模式

- 信任權威：中心化的WEB（現有互聯網）由政府/公司提供服務。
- 無信任：去中心化但需要全局共識的對等網路，比如比特幣。
- 主權個人信任網路 Web of Trust：以主權個人為中心的信任網路



對應三種經濟系統

- 信任權威：央行主導的法幣與傳統金融
- 無信任：比特幣（貨幣）
- 個人信任網路：自組織的社區經濟

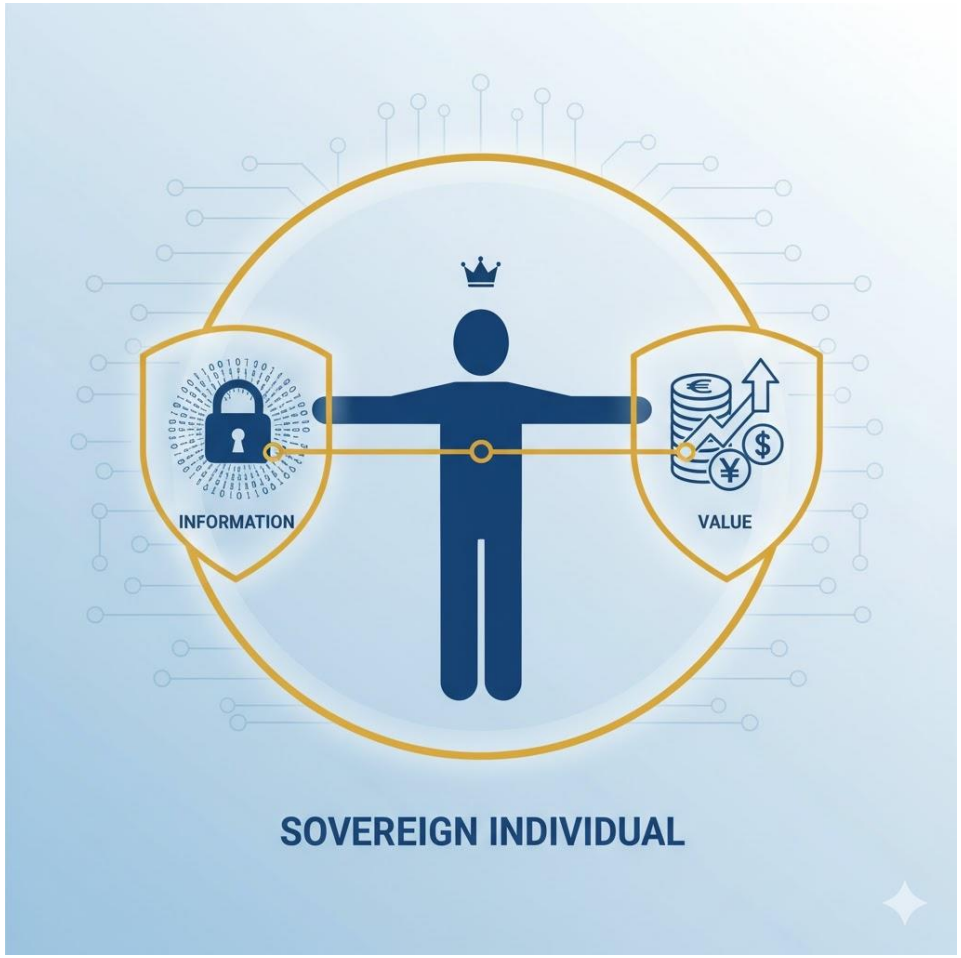
主權個人金融系統

去中心化的比特幣一層做大額清算

很多中心化高效的二層系統做小額的支付/交易/共享經濟

主權個人有完全的獨立性和控制能力

- 價值主權
- 隱私交易



資訊與價值自由
可以很快實現

謝謝