Cyber Chemistry

Exciting Possibilities in the overlapping of material science and computer science

Gideon Samid

EECS500 Fall 2019 Department Colloquium

September 24, 2019

Cyber Space Moored to Chemistry

- The Digital Realm is vulnerable. The most sophisticated data shops were seriously violated.
- Patchwork is not enough.
- A Fundamental Approach is Needed.
- **Mooring Cyber Space to Material Identity**

Identity

- Digital Entities have values, but have no identity. Alas, humans assign identity to digital beings, which is what criminals abuse.
- Material Entities may, or may not, have values, but they always have an identity (talking about macro reality).
- ***By Linking Chemistry to Cyber we will impress identity on digital items, and prevent fraud***.

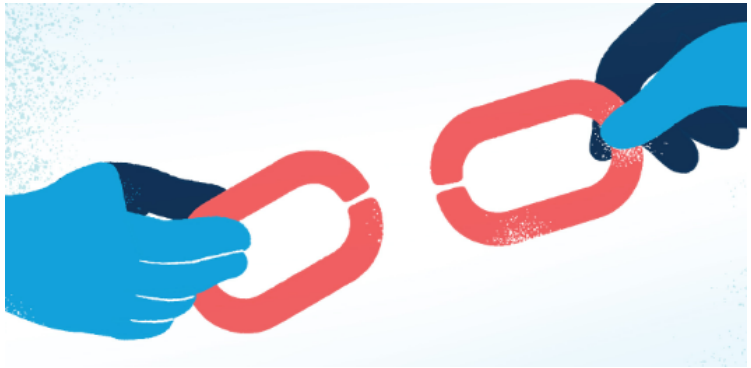
How to Link Chemistry to Cyber?

- **Sourcing**

Using Chemistry to project identity on digital entities.

- **Fencing**

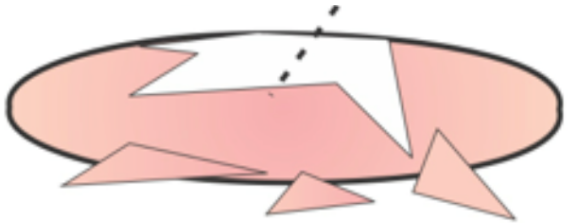
Using chemistry to fence-off digital entities against fraud.



Fencing

- **Brittle Enclosure**

Housing electronic data is an egg-shell like envelope, where tampering is clearly visible.



- **Tamper Resistant Enclosure**

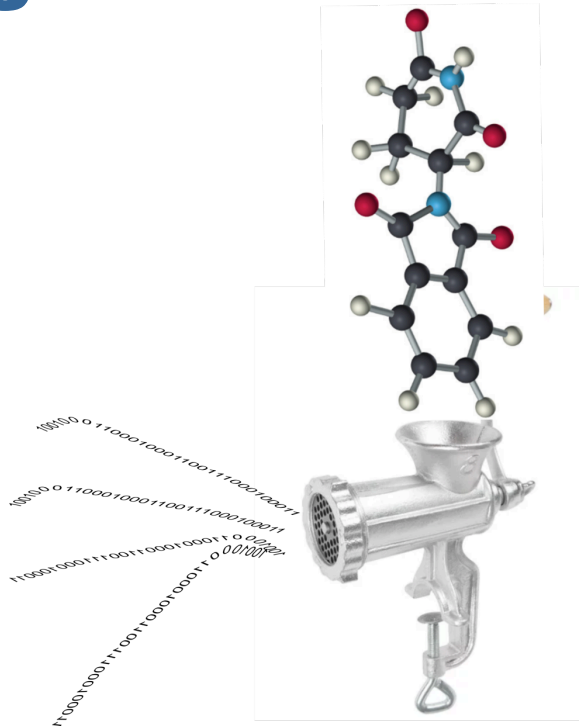
Keeping data 'live' so it is 'killed' upon detection of an assault on its envelope.

Detecting Tampering

- Light
- Pressure
- Absorption

Sourcing

- Extracting Digital Entities from the Chemistry of Matter.
- The identity-bearing chemical source is always there to neutralize fraud and deception.

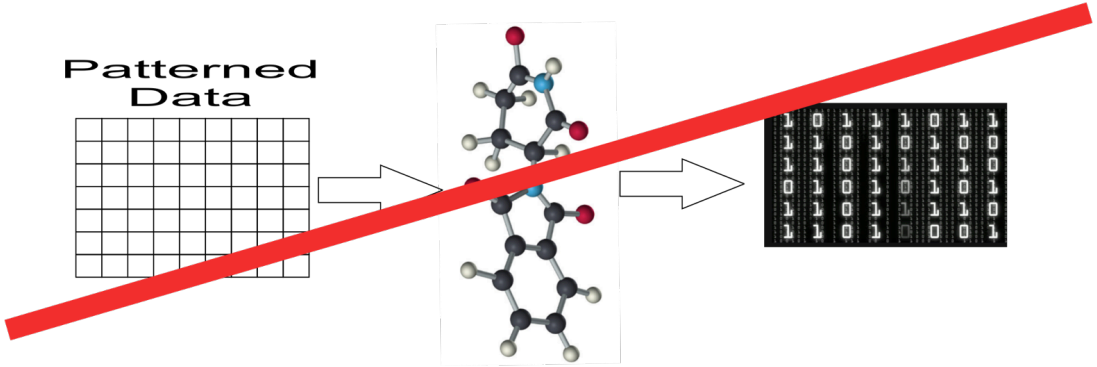


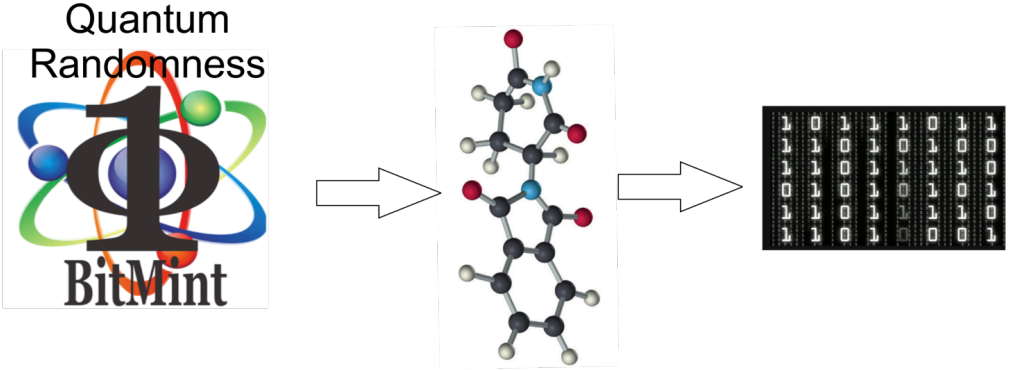
Chem to Cyber

- The One-Way Requirement: Cyber-to-Chem Infeasible (for specific applications).
- E.g.: **Safe Cash at any Denomination**

Quantum Randomness

- **Security without quantum randomness is insecurity.**

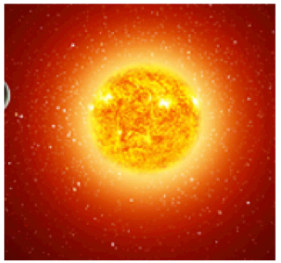




Randomness: Cyber Oil

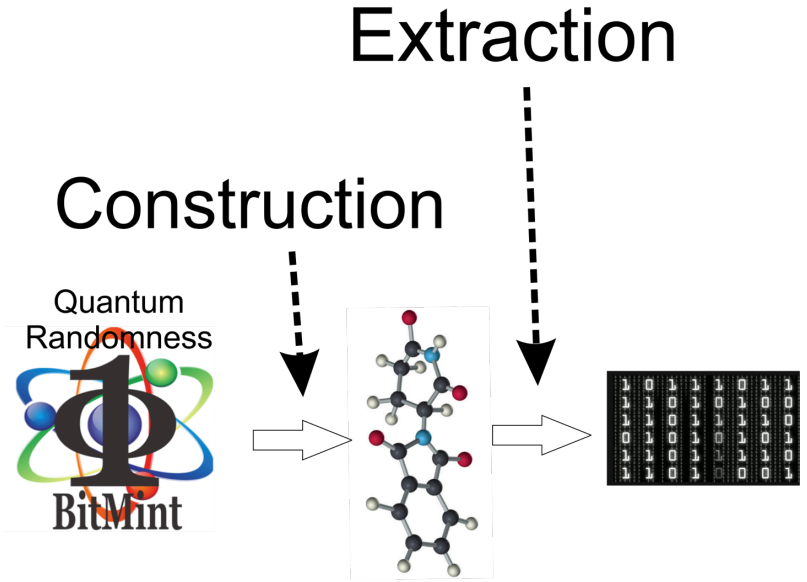
- Oil at the core of Earth was tapped to power up 20th century civilization

- Randomness at the core of Reality is now being tapped to power up 21st century cyber civilization.



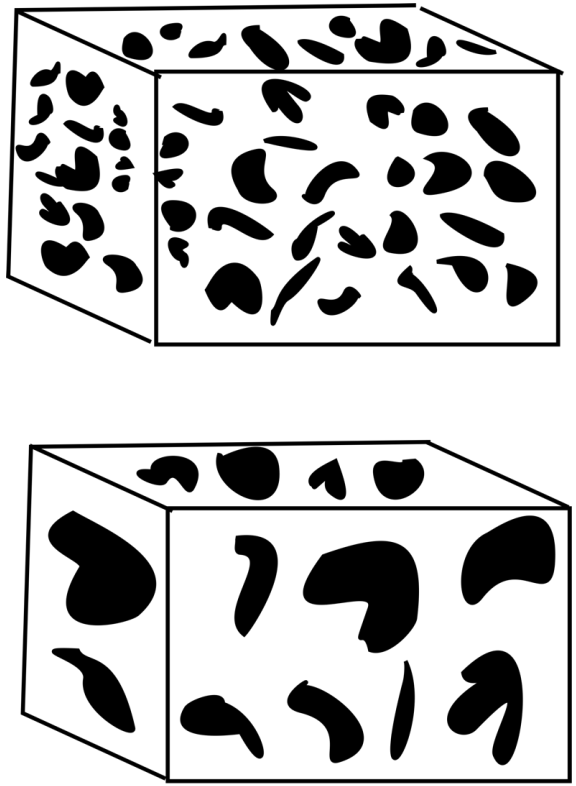
Construction, Extraction

- This is a fertile challenge for which an interdisciplinary effort should be brought to bear. A rare opportunity to lead the way in a field that is so critical for making our new cyber home more habitable.



Entropic Alphabet

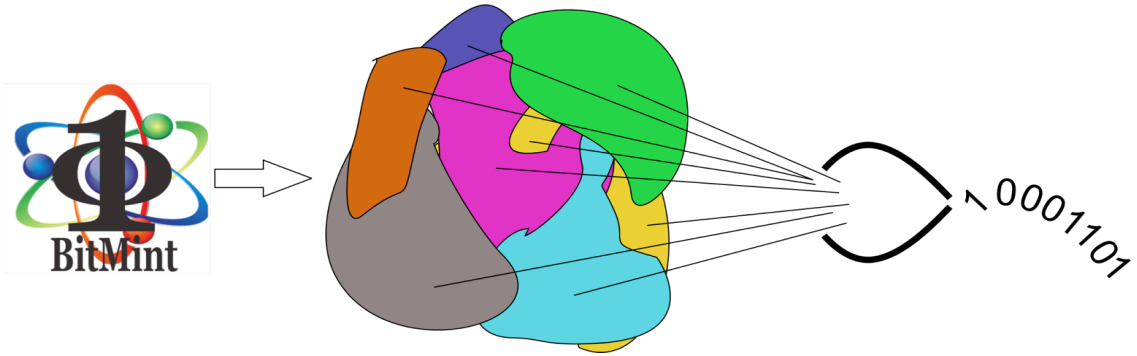
- “Soaking” a 2D message into a 3D lump – making it universally readable, and unforgeable.
- Letters are marked and read by area degree of randomness.
- Using new metric for degree of randomness based on absence of symmetry.



Entropic Alphabet

Current Solution

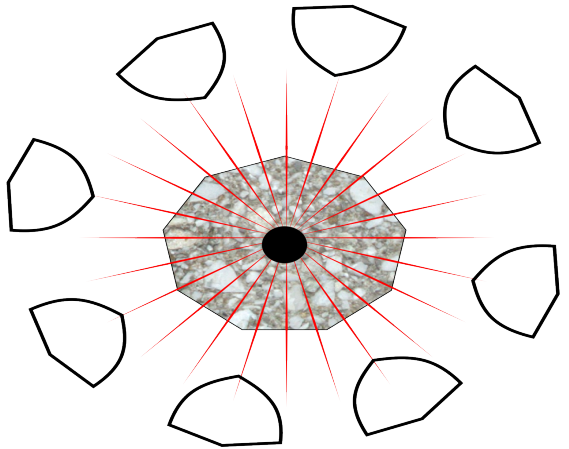
- Randomly assemble n constituent materials of distinct properties which can be measured superficially, and take a non-invasive integrated measurement of the assembled lump, where the reading reflects the randomized assembly, which is therefore equally randomized.



Radiation Absorption

- Constructing a lump from constituent materials of variant absorption of a specific electromagnetic range, placing a central radiation source, reading external radiation at well configured locations.

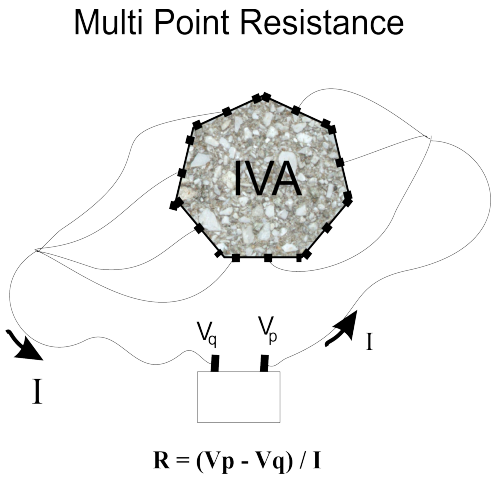
Built-In Central Radiation Source IVA



Conductivity Method

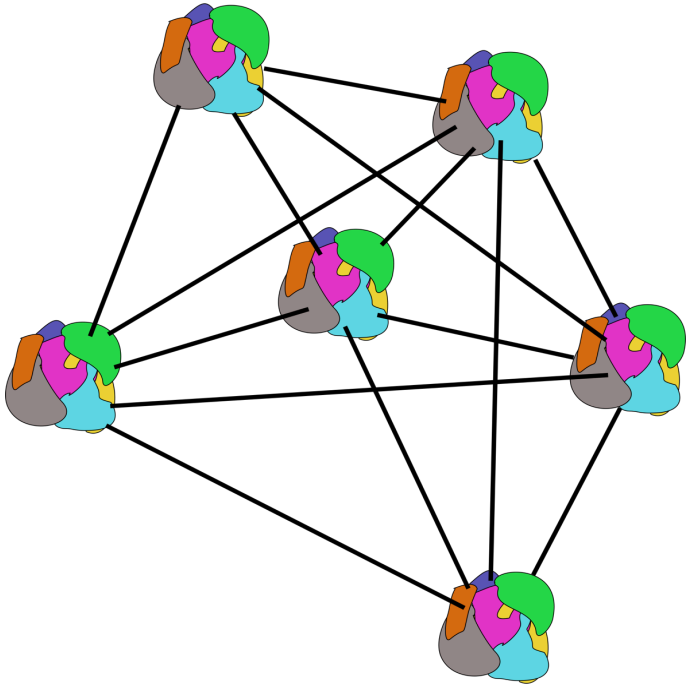
- Fit n electrical ports on the face of the lump assembled from randomized zones of variant electrical conductivity.
- Connect a group of p ports with potential Vp, and a group of q ports with potential Vq.
- Measure lump resistance: R(p,q) = (Vq-Vp)/I
- Very large number of randomized measurements:

$$N = \sum_{q=1}^{n-1} \sum_{p=1}^{n-1} C_n^p \, C_n^q$$



Network Security

- Network nodes using duplicates of a “**Rock of Randomness**” will communicate securely.



Trans-Vernam Ciphers

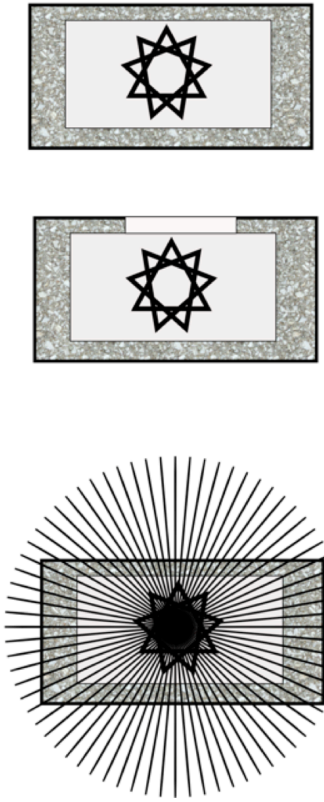
- User responsible for security of her data by deciding how much randomness to use, up to mathematical Security.

IoT Security

- Standard Cryptography is a battery-hog.
- Randomness Based Cryptography is battery-friendly.
- Small ‘rocks of randomness’ fitting in tiny devices.

Material Identity

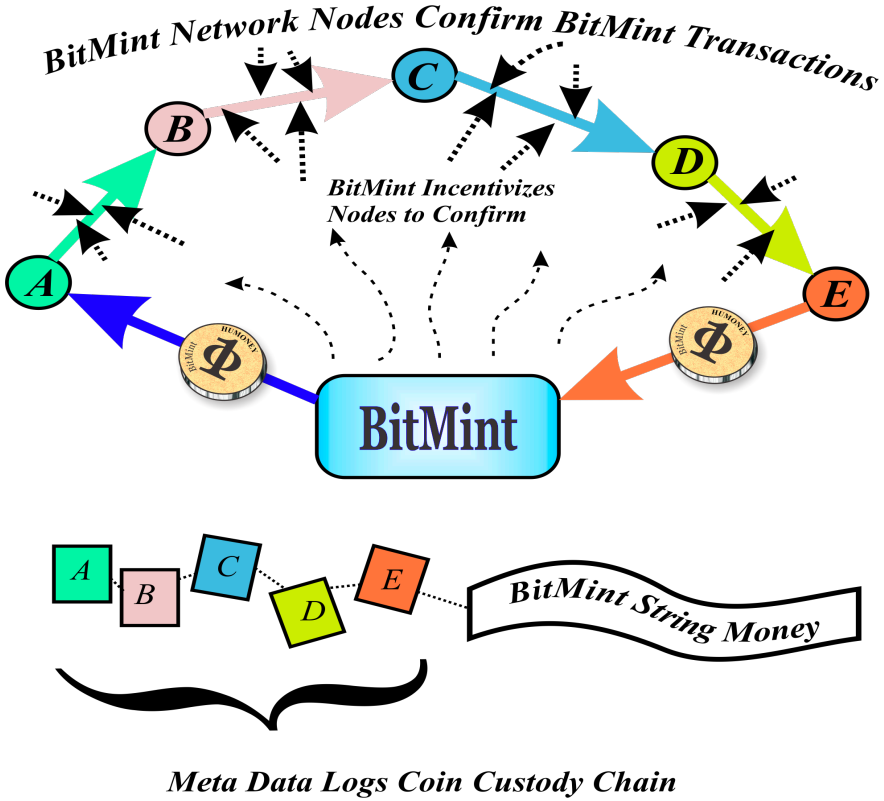
- Published Ledger of Tracked Articles
- Local Readings to Verify Identity
- Network Connectivity Not Needed



21st Century Cash

- Extracting Digital Identity from Cyber Chemistry.
- Minting Tethered Money, giving the National Financial Surgeons a fine scalpel to Operate on the economy (replacing the sledgehammers of the 20th century).

Centralized, Switchable Anonymity, Randomness Security

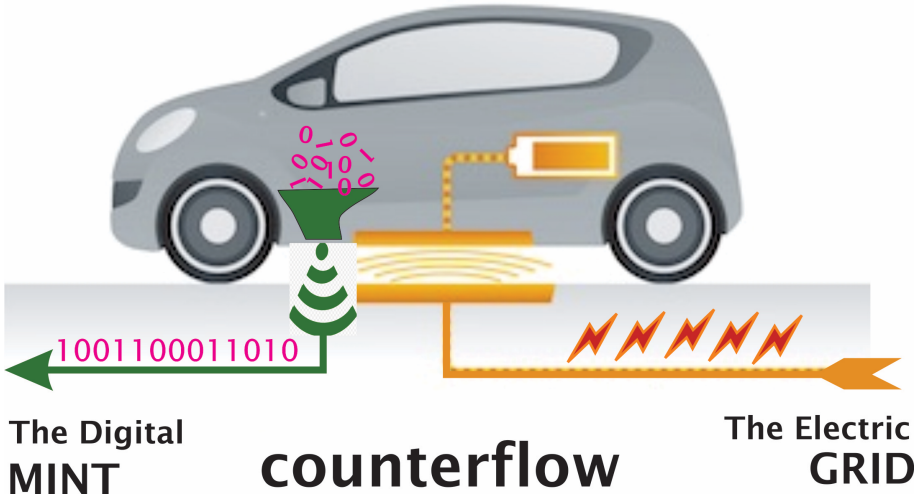


Meta Data Logs Coin Custody Chain

Trader A buys a BitMint digital coin, passes the coin to trader B; B passes to trader C, then to D and E. E redeems the coin with BitMint.

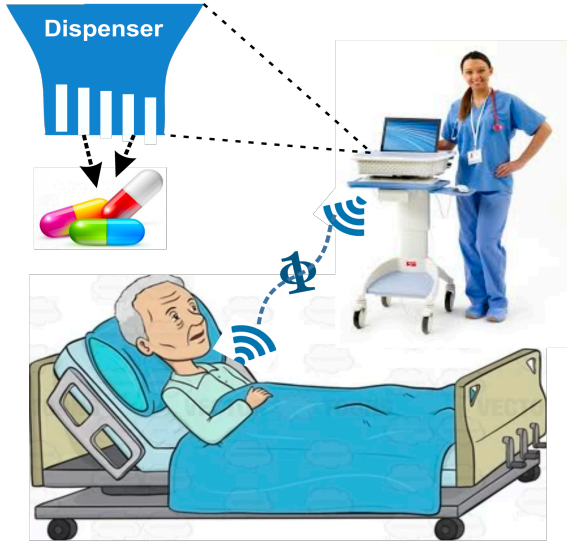
New Realms of Payments

- Chem-Randomness powered digital money fuses identity and value, allowing very fast, very small payments to occur where they could not have occurred before.

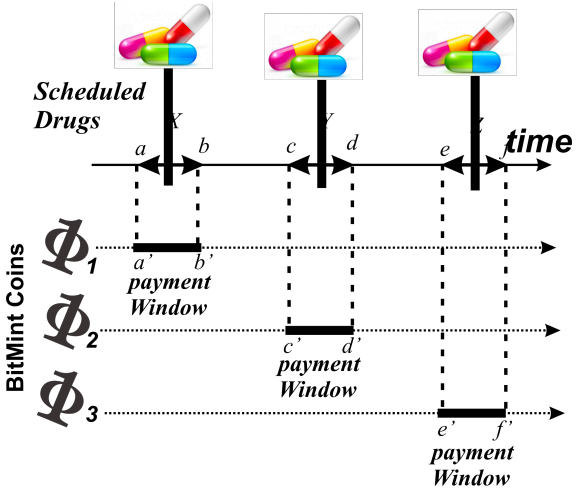


High Resolution Enables Error Prevention Tracking

- Chem-Randomness Money is open-ended resolution payment regimen, enabling pay-as-you-go, which allows tracking of performance v. expectations, to spot errors and abuse.

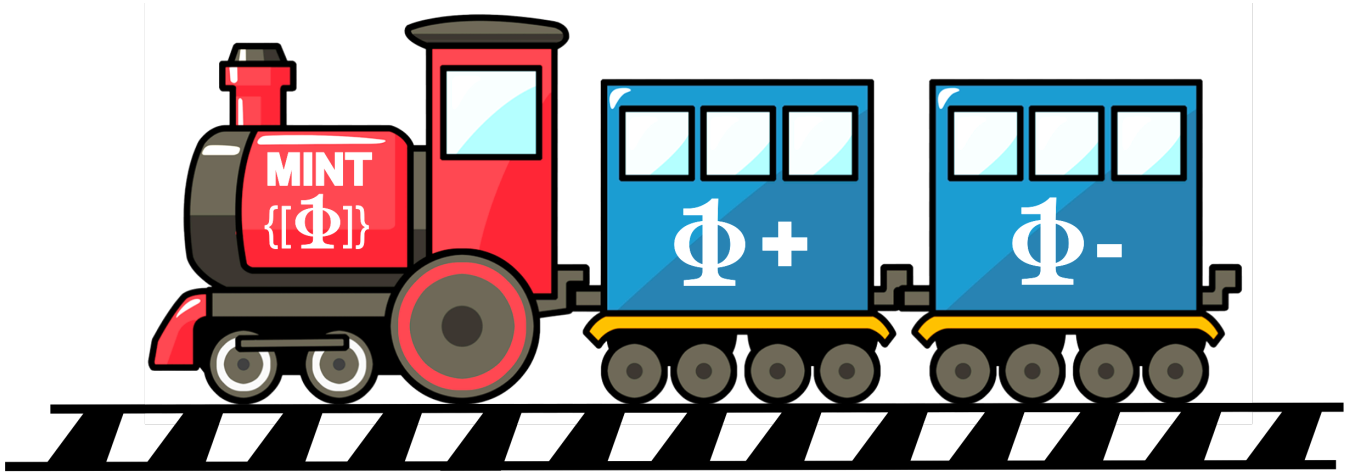


Patient pays-per-pill,
Nurses work less, Fewer Errors



Pay-Per-Pill Helps Patients Take their Prescription Drugs on Time

Extending Chem-Randomness to Any Financial Entity

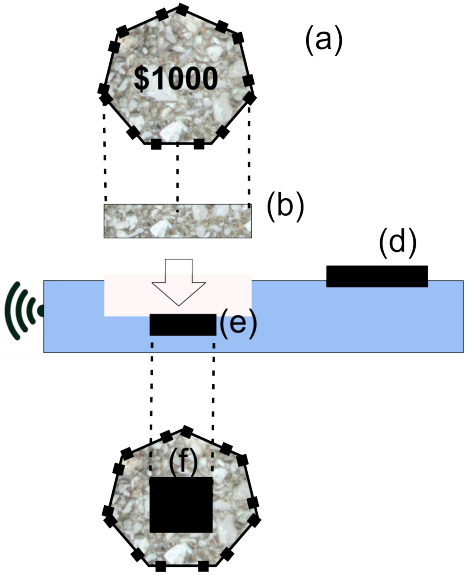


BitMint Financial Railways Transport Positive and Negative Cash

Payment Continuity

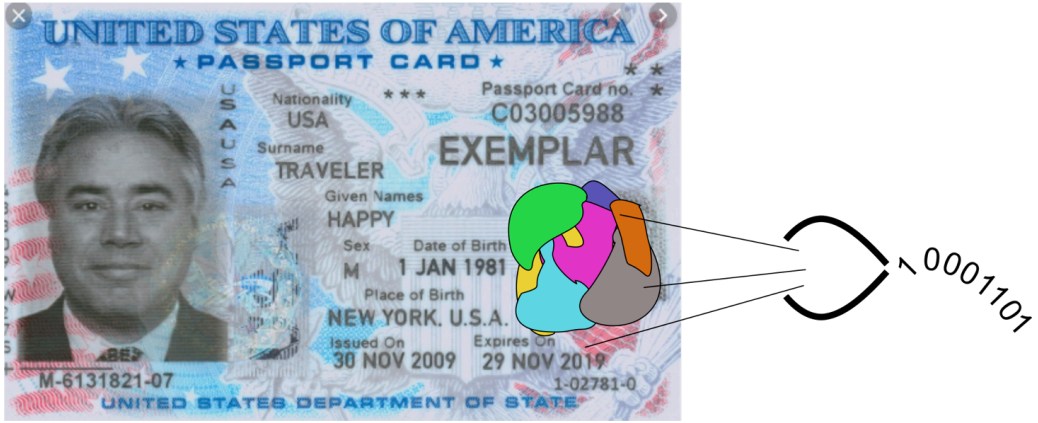
- Chem-Randomness BitMint Physical Coins are payable between two battery-operated devices, when the Internet is down.
- Payment continuity is indispensable for national level digital currency.

Coin Logger Side View



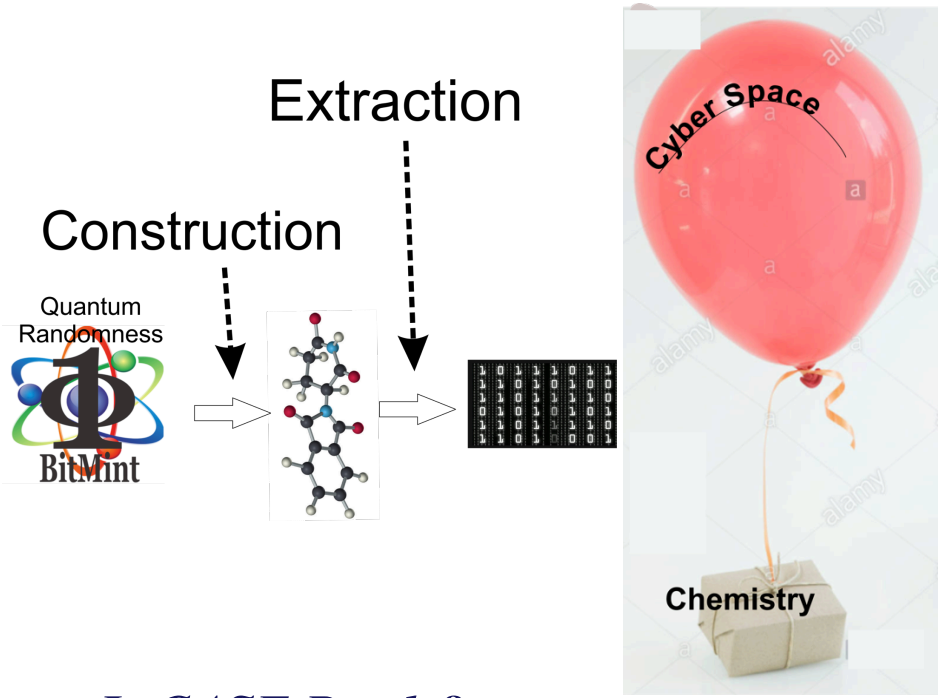
Personal Identities

- Public Ledger of Citizens' Randomized Signature reveals no personal data, but prevents identity theft.



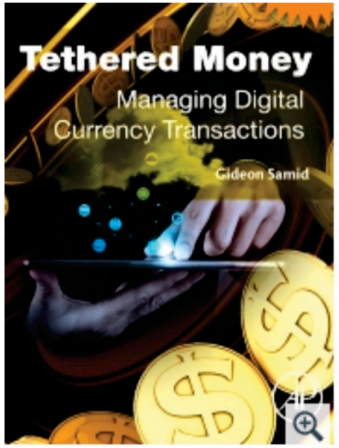
Outlook

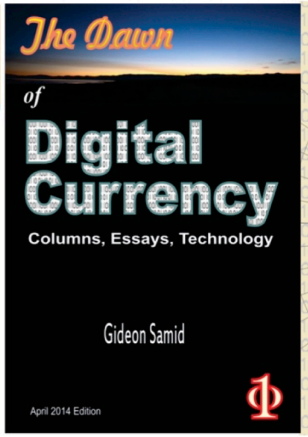
- This is a fertile challenge for which an interdisciplinary effort should be brought to bear. A rare opportunity to lead the way in a field that is so critical for making our new cyber home more habitable.
- BitMint engages in implementation projects of its current technology, but the field requires a long range academic investigation.

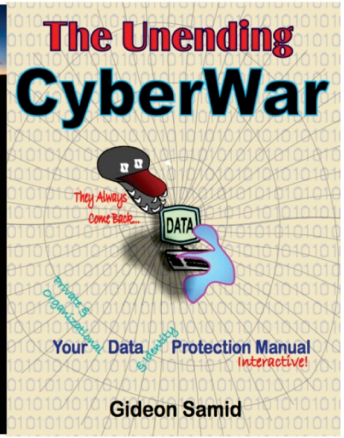


Is CASE Ready?

Thank You for your Attention!







Gideon@BitMint.com
Gideon.Samid@CASE.edu