

GOLD DIGR White Paper - 2023

Broward Horne, Vancouver, WA

browardhorne@gmail.com

<https://broward.ghost.io>

I'm a software developer with 30+ years of experience. For reasons listed here, there may soon be demand from State governments for R&D, prototyping and development of gold-backed digital currencies as described in [Texas bills S.B. No. 2334 and H.B. No. 4903](#). I'm seeking a related contract position.

Abstract:

This white paper provides an overview of a **GOLD**-backed **DIG**ital currency (**GOLDDIGR**) using blockchain technology and backed by a State precious metals depository. It outlines historical forces, strategic design, key features and technical issues to familiarize readers with core concepts and impacts.

Immediate Considerations

Low Energy Use:

GOLDDIGR does not require enormous energy. It consumes the same energy as sending an email or editing a document. Most crypto-currencies refer to "mining", "Proof of work", "consensus mechanism", etc, which are energy-intensive features to create artificial scarcity. GOLDDIGR's scarcity is the gold depository.

Low Complexity:

GOLDDIGR is less complex than crypto-currencies. It doesn't require "proof" schemes to generate scarcity, validation and consensus mechanisms, etc.

Political Issues

- Is cash equivalency a goal? A defining trait of cash is its **lack of identity**.
- Is Regional Interoperability a goal?

Design Issues

The most complex and controversial areas are

- **key management** (similar to safety deposit box keys)
- select an appropriate **blockchain**,
- **integration** of blockchain with existing inventory system
- Determine SLAs for uptime and response time
- Determine peak concurrent users, transactions
- Determine a client/wallet definition

Relevant History

Overview

This period of fiat currency has already lasted longer than previous fiats of the past several hundred years and contrary forces are aligning to end it. Russia and China have planned for the end of fiat for the past fifteen years, the US dollar is ripe, age-wise, for replacement as the world reserve currency, and the current Federal debt is unsustainable.

Gold Standard

The longest period in modern history without a gold standard is now; from 1971 to 2023 or 52 years. The last major gold standard system was the Bretton Woods system, which operated from 1944 to 1971. The United States has abandoned its gold standard in unusual situations (Civil war, World War 1, etc) but only for a few years.

Russian Gold Reserves

Since 2009, Russia's central bank has steadily increased gold reserves to diversify away from the US dollar and foreign currencies. According to the World Gold Council, Russia's gold reserves more than tripled from 600 metric tons in 2009 to over 2,300 metric tons in early 2021.

Chinese Gold Reserves

China has consistently increased gold reserves since 2009 to diversify away from US dollars and foreign currencies, according to data from the People's Bank of China (PBOC). China's gold reserves grew from 1,054 metric tons in 2009 to over 1,948 metric tons in early 2021.

Hegemony

Western hegemonic empires since 1400 A.D. had an average lifespan of 95 years and the United States has already exceeded that. The world reserve currency is usually a function of the current hegemony. No hegemony, no reserve currency.

Country	Dates	Duration
Portugal	1450 to 1530	80
Spain	1530 to 1640	110
Netherlands	1640 to 1720	80
France	1720 to 1815	95
Great Britain	1815 to 1920	105
United States	1920 to 2023	103

Interest Payments

The current rate of increase in [Federal debt interest payments](#) is unsustainable.



Federal Interest Payments

Interest Rates

As debt increases, rates must fall to maintain equilibrium. Interest rates during the credit upcycle (1980 to 2020) have fallen as far as investors will tolerate. The inevitable return of higher rates will be disastrous for the current debt.



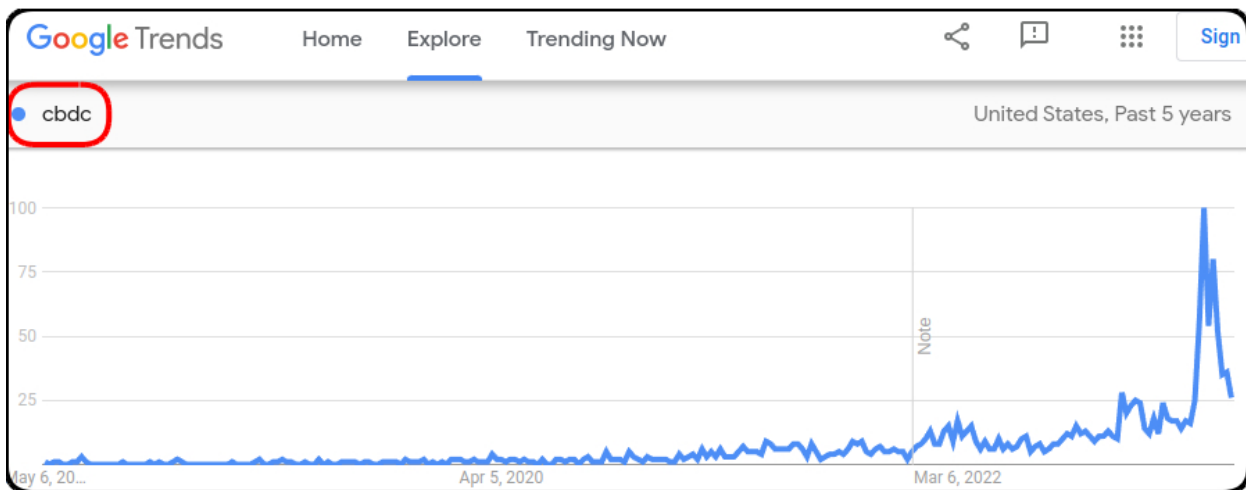
BRICS Strategy

De-dollarization. The BRICS separate financial system aims to use their oligopoly power to control commodity prices and bypass the US Dollar. BRIC countries control 1/2 of the world's food supply, most of the microchip supply (assuming China invades Taiwan) and enough energy to control pricing in concert with a partner like Saudi Arabia or Venezuela.

A	B	C	D	E	F	G
	Oil	Natural Gas	Wheat	Rice	Fertilizer	Microchips
Russia	17	24	10		18	
China	6	3	19	30	12	20
Ukraine			4.5			
Iran	3	16	1.5		1	
India			15	23		
Taiwan						50
	26	43	50	53	31	70

Central Bank Digital Currencies (CBDC)

Interest in CBDCs and development has accelerated in the past year. CBDCs centralize power and control of a currency which could lead to potential abuses, restrictions, or even political interference in financial transactions.



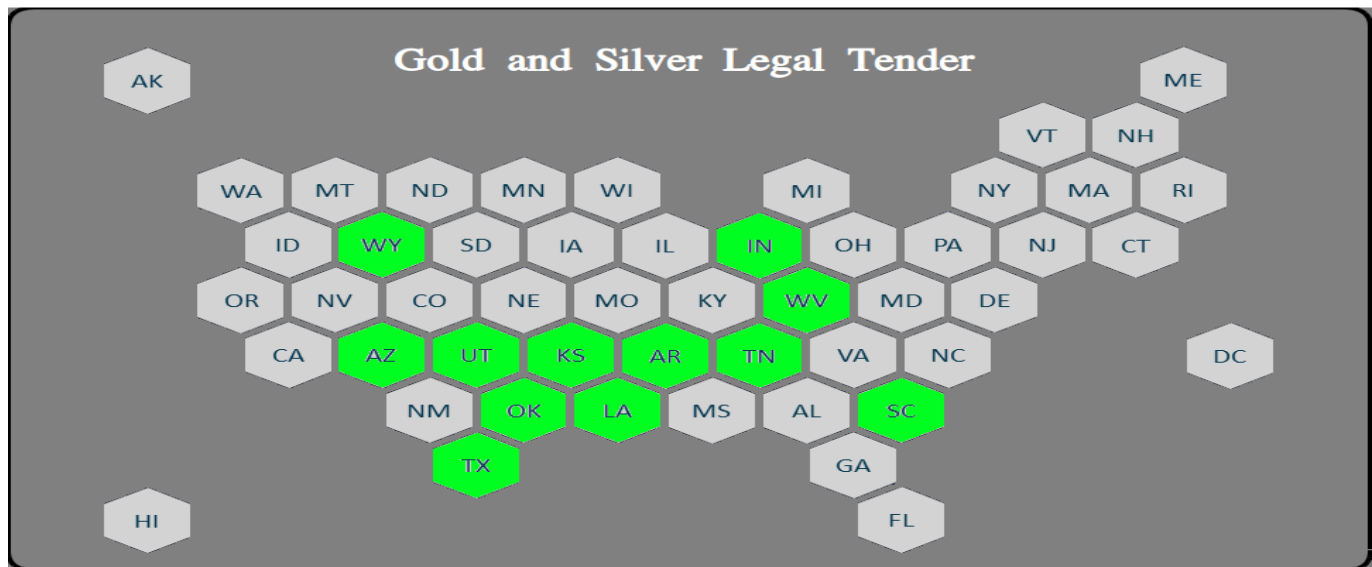
USA Legislation

The **Sound Money Movement** is a [political and economic movement](#) that advocates for a stable, reliable currency and believes central banks should not manipulate currencies for political gain and that a gold or silver-based currency would provide greater stability. The movement supports precious metal legislation across the United States.

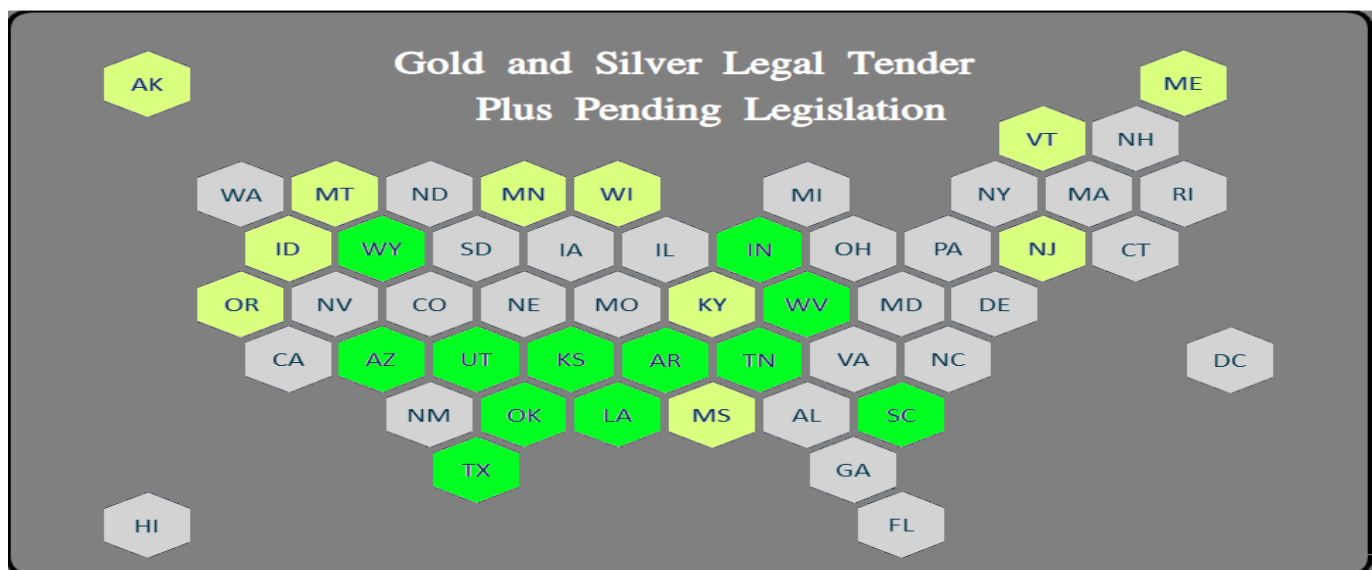
Three-Step Legislative Strategy

1. Pass legislation to legalize gold and silver-based
2. Create a State-controlled precious metals repository
3. Create a digital token currency backed by the repository

1) States where gold and silver are legal tender



2) Plus States with pending legislation in 2023



Previous Depository Legislation

Texas Bullion Depository Bill - signed into law in 2015 and authorized the creation of a state bullion depository.

Tennessee Bullion Depository Act - In **2023**, SB 150 would establish a precious metals depository.

Arizona Gold Bonds Act - introduced in **2021** to create a state-run gold depository

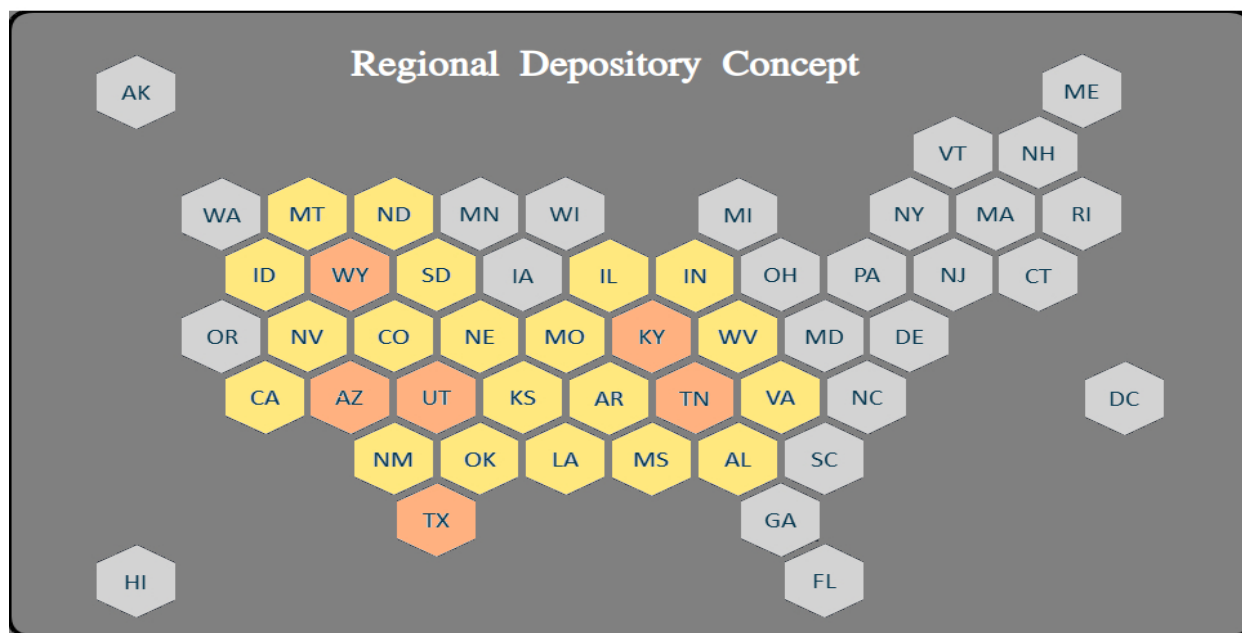
Utah Sound Money Amendments - introduced in **2021** that would authorize the creation of a state bullion depository.

Kentucky Precious Metals Depository Act - introduced in **2021** to authorize the creation of a state-run precious metals depository.

Wyoming bullion depository, 2020 - provided for the creation and administration of the Wyoming bullion depository

Regional Depository Concept

If the previous legislation had passed, our depository map would look like this and Depository States (gold) could support regional currencies of non-depository States (yellow).



Considerations

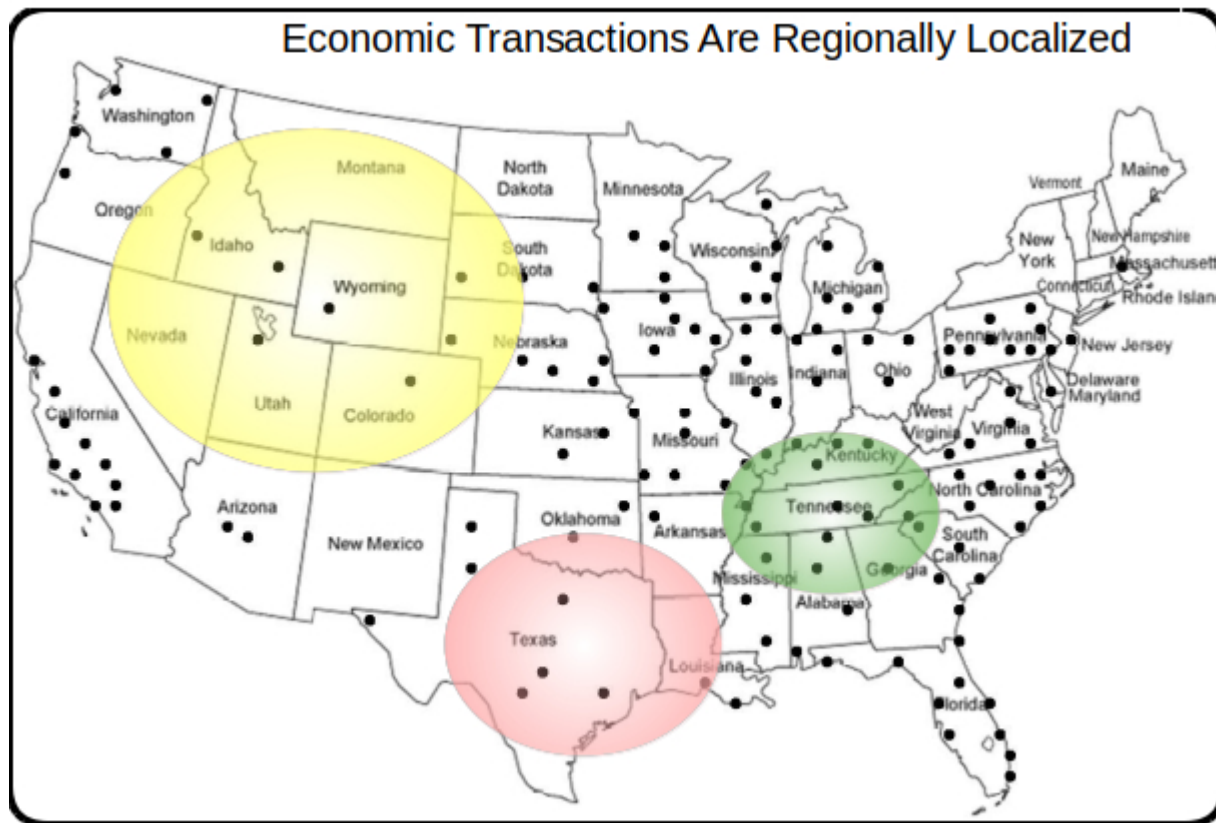
- depository holds bullion only (for fungibility)
- interoperability with other depositories
- is ACH (Federal Reserve) access necessary?

Regional Coordination

coordinate State laws, implementation, settlement schedule, delivery and security, reciprocity with adjoining States

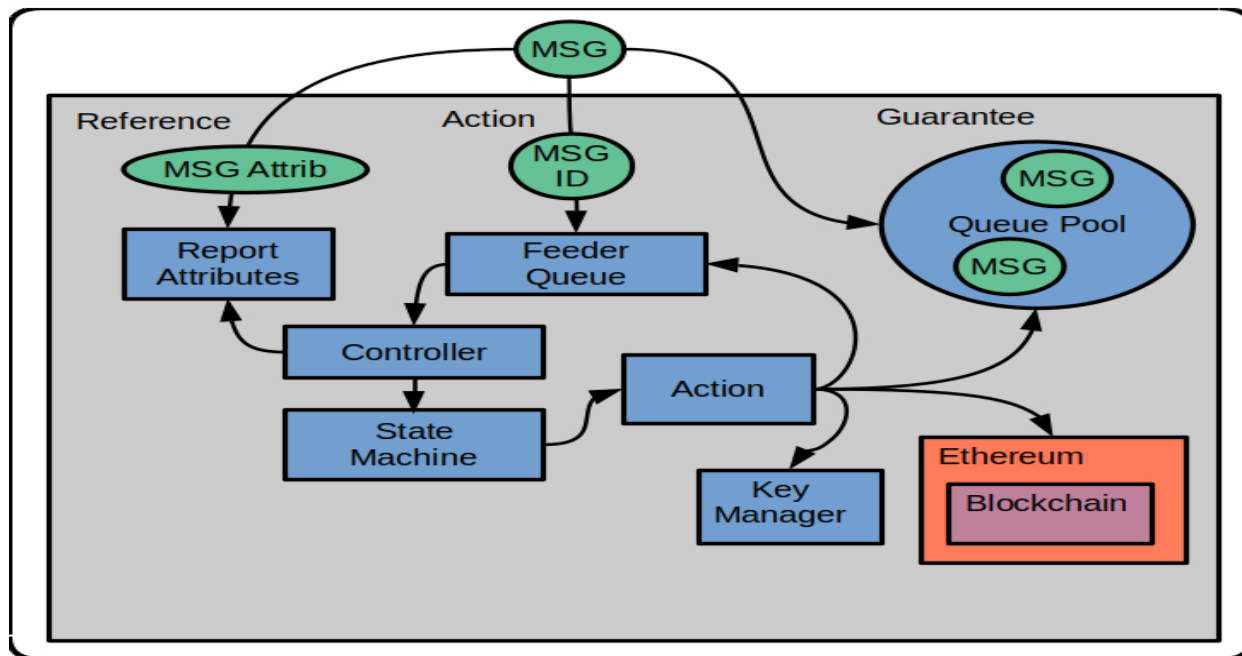
Impedance-Matched Currency

Creating the Euro was somewhat like harnessing a horse, a mule, a dog and a turtle to pull a wagon. A "one size fits all" strategy creates stresses because regions (States) have different resources, skill levels, goals. Most economic transactions are local and a regional currency would be controlled regionally.

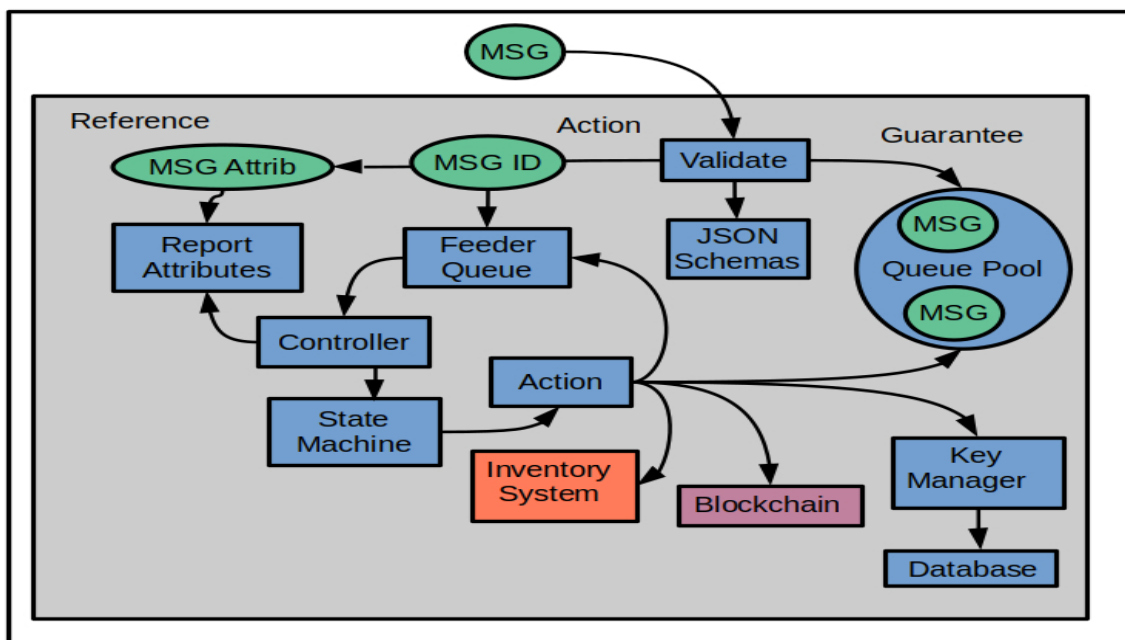


Proposal

In 2018, I wrote a successful crypto-currency platform on Amazon AWS, [Sila stablecoin](#). Our goal was to help hundreds of 3rd party developers easily add crypto capabilities into their phone apps. This is an improved design I sketched out in 2020.



The proposal is to replace the Ethereum component with a separate blockchain and optional Gold Depository Inventory System. This design would be very similar.



More technical detail at Strategy

More technical detail on AWS Implementation

Strategic Design

This is an abstract high-level diagram of how a gold-backed digital currency would work. A detailed design is at <https://broward.ghost.io/golddigr/tactical>

Depository: stores gold deposits.

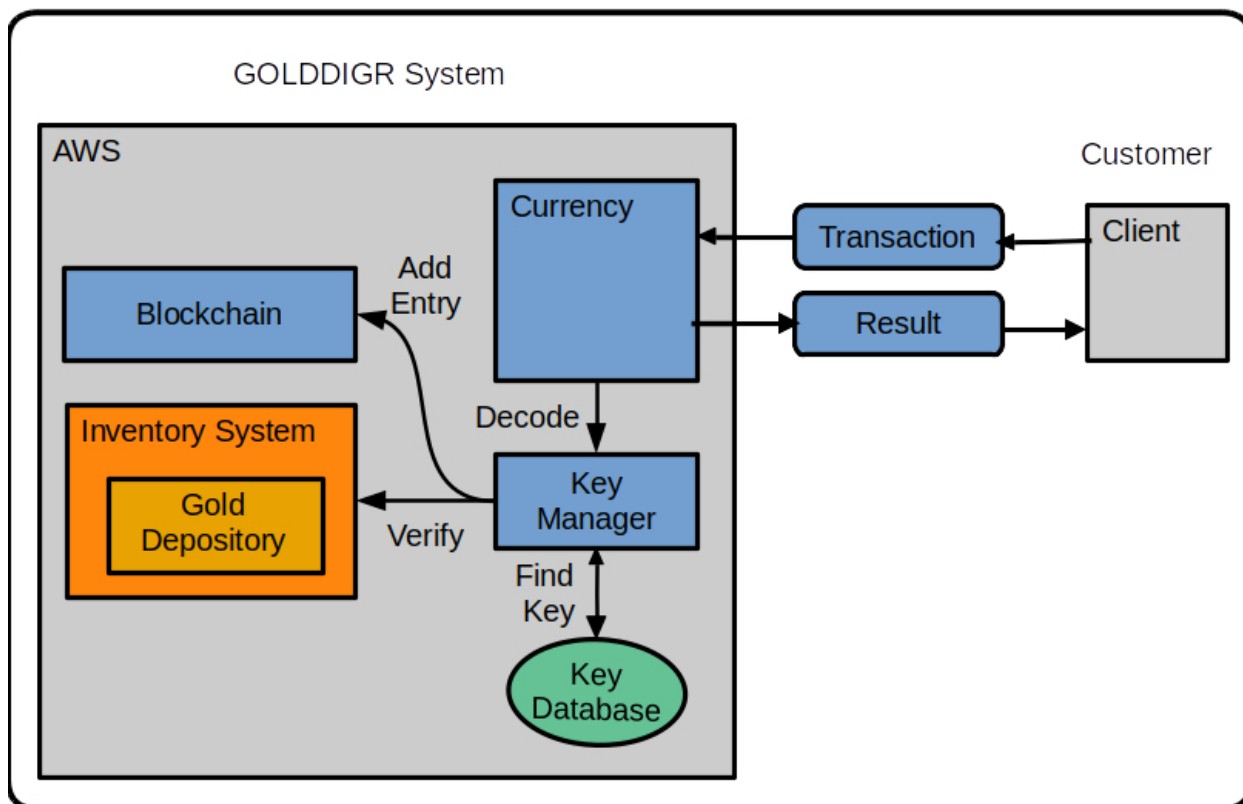
Inventory System: manages gold deposits

Currency: manages cash transactions

Blockchain: equivalent to accounting ledger

Key Manager: equivalent to safety deposit box keys

Client: Customer with gold in depository



Assumptions: An existing depository has an existing inventory management system. That system needs to synchronize with the blockchain entries. The inventory system may be usable as the currency blockchain but it's to be determined.

Sending A Transaction

1. Client sends a transaction to Currency API

Example message:

```
{  
  "message": {  
    "message_type": "texas_transaction",  
    "version": 1.12,  
    "date": "2024-02-03T06:48:07",  
    "ID": 010102283,  
    "payer": 12221,  
    "payee": 1023,  
    "amount": "$100"  
  }  
}
```

2. Currency forwards message to Key Manager.

3. Key Manager verifies the payer, payee and payer's balance.

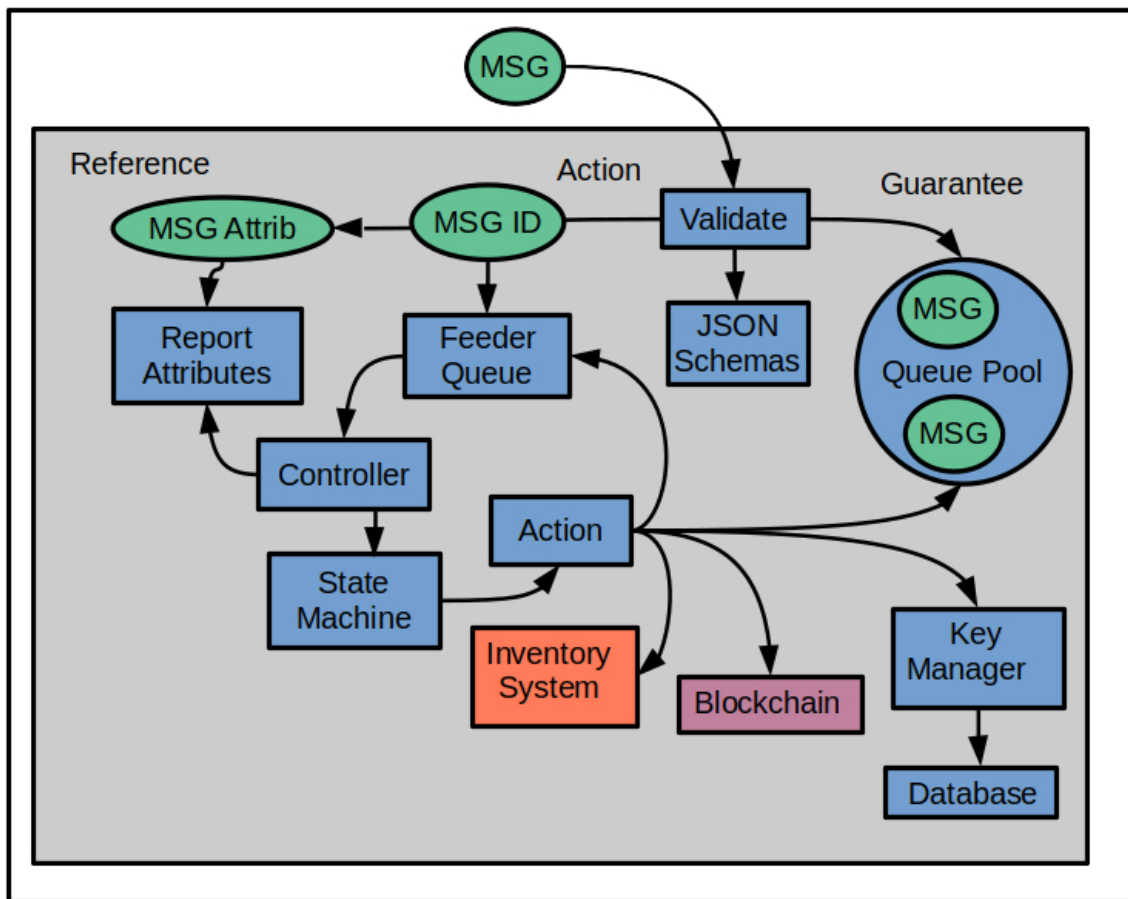
4. Key Manager creates blockchain entry and sends result to Currency.

5. Currency sends result to client.

More information on [technical details](#)

More information on [AWS implementation](#)

Tactical Design



Three internal domains defined - Guarantee, Action, Reference.

Incoming message is validated with ECC decryption of signer ID. JSON schemas enforce a language-agnostic message definition for 90 to 95% of validation rules. Code functions validate 5 to 10%.

Guarantee uses AWS SQS queues to guarantee state and execution. Stores the ECC-signed message in its own queue named by unique Msg_ID. This is the only place the original message exists until it is archived.

The **Action** Lambda function accepts Msg_ID and adds it into the feeder queue. The controller pulls feeder entries, retrieves the current state of Msg_ID. Current state is fed into state machine which executes the next action. The action pulls the original message, executes, then updates Msg_State. The Msg_ID is re-submitted to the feeder queue for the next iteration through the controller until End_State is reached.

The **Reference** Lambda receives a subset of message attributes for reporting/tracking purposes, such as creation_date, client_id, etc. The original message is immutable except for Msg_State. The controller updates Reference with current state before each iteration. Complexity is mostly isolated in the State Machine/Rule Engine, so most future changes are there. The rest of the system should be stable, needing few changes except the addition of new actions.

My original design should have had an entry API to issue a unique Msg_ID. This is the initial client call which returns Msg_ID, client adds it to the transaction message before it's signed, making it part of the immutable structure. The Msg_ID has a timestamp and time frame of a few seconds to send the transaction message.

There's duplicate data between the three domains, Guarantee is the system of record if we get a data mismatch. There's also a need to store temporary data which may get passed from action to action, so add a Msg_Ext message to the queue. There's a coordination issue we can solve with Json schemas.

AWS Cloud Formation, https://broward.ghost.io/ /aws_app_1/

Messaging, https://broward.ghost.io/ /aws_app_2/

Security, https://broward.ghost.io/ /aws_app_9/

Author

Overview:

Thirty-four years of eclectic software development, including seven startups, IT staff at a major university, several USDOT grants and fifteen years of corporate consulting. Three DEFCON presentations on predictive analytics.

State governments

From 1991-1996, I was the original architect in several Federal Highway Administration grants developing the [first handheld and wireless systems \(ASPEN, CDLIS, ISS\) for State-level motor carrier inspections](#). I led a quarterly design conference with representatives from ten States to define features and recommendations and worked directly with State managers, IT staff and police officers, often on-site. We achieved a 40-State adoption of this software.

Digital Currencies

Hands-on work with three currencies - the Digital Money Trust in 1994 (a precursor to Bitcoin), an IoT token prototype in 2014 and [Sila stablecoin in 2018](#) which received \$21 million in venture capital. I developed the MVP (minimum viable product) in 100 days and we used it in 50 demonstrations for funding. I designed and wrote about 75% of the original beta release code, API, security.

Contracting

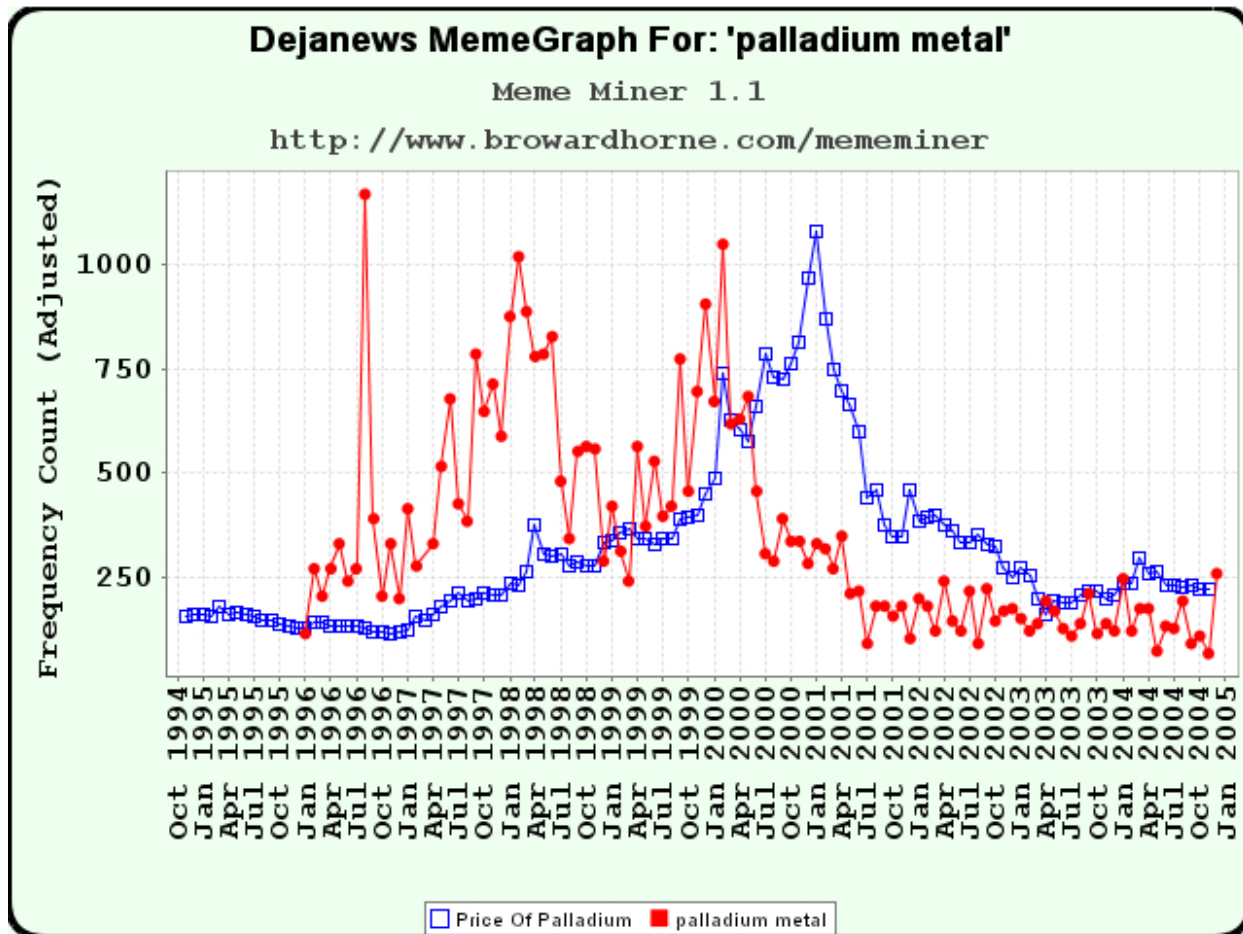
Significant projects at Boeing (call center), Avnet (e-commerce), Aetna (case management), Amdocs (payment system), DLVR.com (video analytics), Verizon (ring tone sales), Staples (e-commerce). Many run one million+ transactions per day and had requirements for internal integrations, adapters and legacy limitations, etc.

DEFCON

Three DEFCON convention presentations in 2005-2007 on predictive analytics and memetic manipulations such as election hacking.

Personal

I bought my first Krugerrands in 2003, my first Silver Eagles in 2004 and I've kept an interest in precious metals ever since. Below is a palladium sentiment graph I data-mined in 2006. See how the sentiment increase (red) PRECEDED the price increase (blue)?



Related Material By Me

- GOLDDIGR White Paper, 2023 (<https://broward.ghost.io/golddigr/>)
- Texas Depository, 2023 (https://broward.ghost.io/texas_depo)
- Stablecoin Hack, 2022 (https://broward.ghost.io/stablecoin_hack)
- Miner Bankruptcy, 2022 (https://broward.ghost.io/miner_bankruptcy)
- Polymorphic API, 2022 (https://broward.ghost.io/polymorphic_api/)
- Bitcoin Death, 2022 (https://broward.ghost.io/bitcoin_death)
- Crypto Platform, 2020 (https://broward.ghost.io/crypto_platform)
- Pandemic and Gold, 2020 (https://broward.ghost.io/pandemic_and_gold)
- Payment System, 2015 (https://broward.ghost.io/payment_system)
- Bitcoin Scalability, 2015 (https://broward.ghost.io/bitcoin_scalability)
- Digital Money Trust, 2015 (https://broward.ghost.io/digital_money_trust)
- Jing Currency on IoT, 2014 (https://broward.ghost.io/digital_on_IoT)