Gold-back Digital Currency White Paper - 2023

Broward Horne, 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 looking for 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 economic forces, strategic design, key features and technical issues to familiarize readers with core concepts and impacts.

Key Issues

Low Energy Use:

GOLDDIGR shouldn't consume enormous energy but the same energy as sending an email or editing a document. Most crypto-currencies refer to "mining", "Proof of work", "concensus mechanism", etc, which are energy-intensive features to create artificial scarity. GOLDDIGR's scarity is the gold depository.

Low Complexity:

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

Cost

In 2018, I wrote a similar crypto platform using Ethereum. In my experience, a production-ready system could be done by a team of five people within one year for under $2 million.

Biggest Variable

In my opinion, the biggest technical variable will be revisions to the existing inventory system at the Texas Bullion Depository. There's more detail later in this paper

Economic Forces

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.

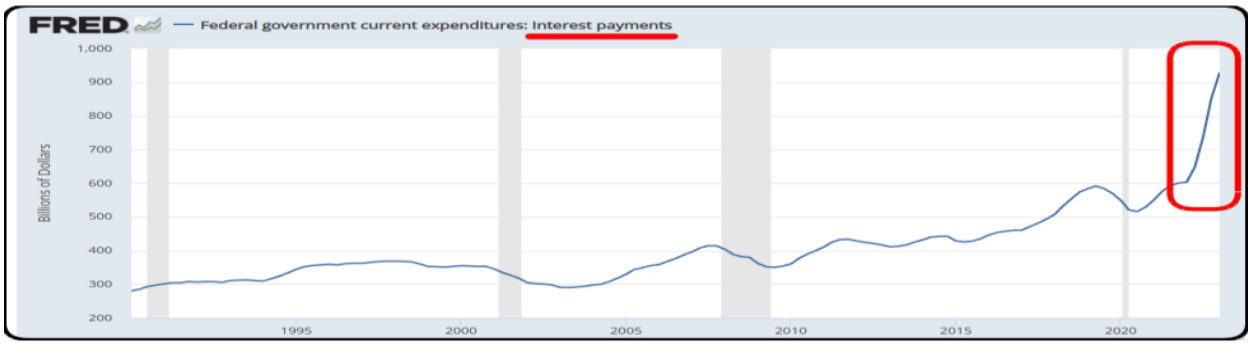
Hegemony

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 years
Spain	1530 to 1640	110 years
Netherlands	1640 to 1720	80 years
France	1720 to 1815	95 years
Great Britain	1815 to 1920	105 years
United States	1920 to 2023	103 years

Interest Payments

The current rate of increase in Federal debt interest payments is unsustainable.



Interest Rates

As debt increases, rates must fall to maintain equilbrium. 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 will 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.

	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 restrictions or political interference in financial transactions.

USA Legislation

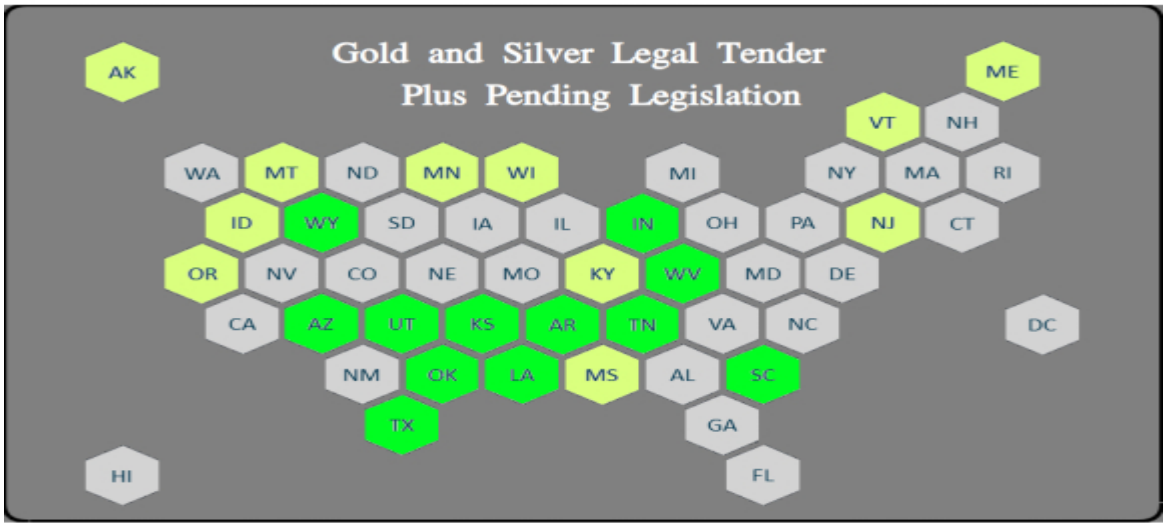
The **Sound Money Movement** is a political and economic movement that advocates for a stable, reliable currency and believes central banks should not manipulate currencies for political gain and that a gold or silver-based currency would provide greater stability. The movement supports precious metal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

Three-Step Legislative Strategy

1) Legislation to make gold and silver tax-free legal tender

2) Establish a State-controlled precious metals depository

3) Create a digital currency backed by the depository

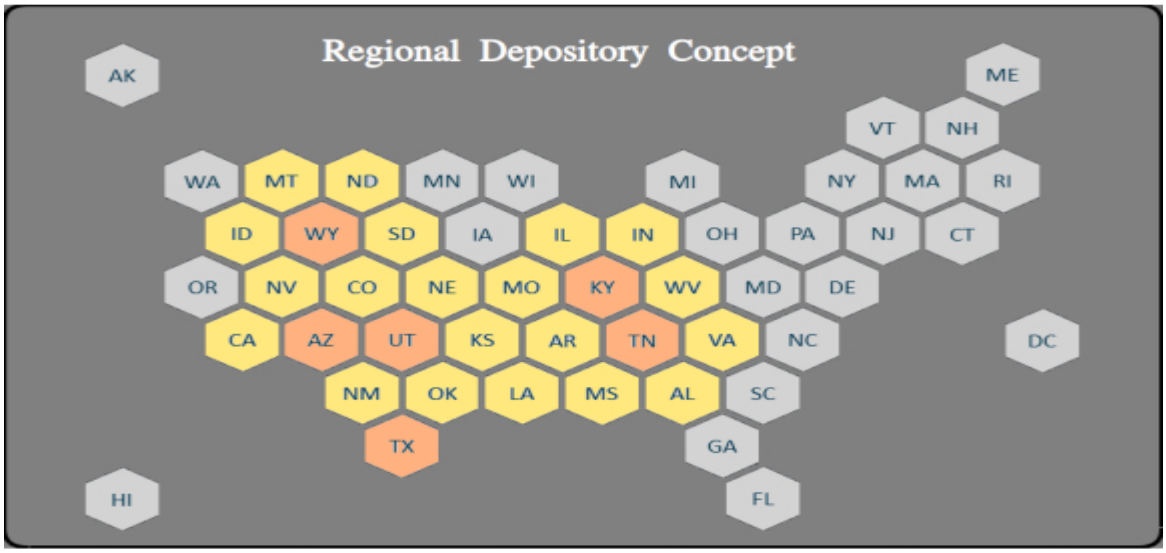


Previous Depository Legislation

Texas Bullion Depository Bill - signed into law in 2015 to createof 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** for creation of a state bullion depository.
Kentucky Precious Metals Depository Act - in **2021** to create a state-run precious metals depository.
Wyoming bullion depository, 2020 - provided for the creation of the Wyoming bullion depository.

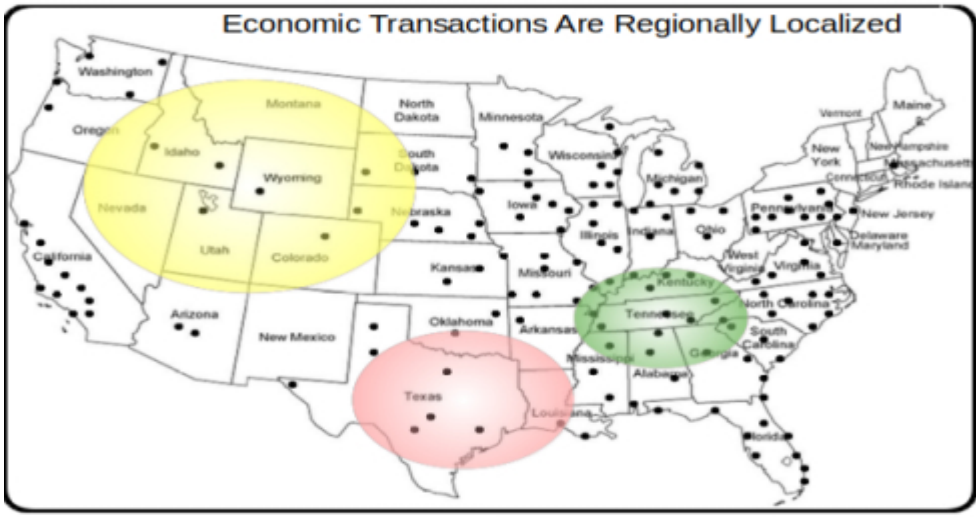
Regional Depository Concept

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).

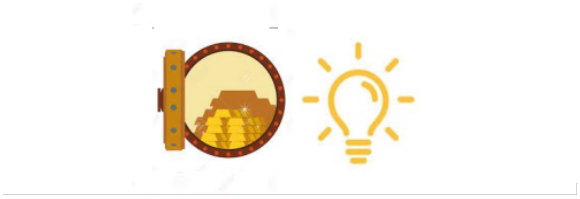


Impedence-Matched Currency

Creating the Euro was 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 histories, resources, skill levels, desires. Most economic transactions are local and a regional currency would be controlled regionally.



Considerations



Design Issues

The most complex and controversial areas are

- cash equivalency
- key management (like safety deposit box keys)
- appropriate blockchain,
- integration of blockchain with inventory system
- KYC validation
- SLAs for uptime and response time
- peak concurrent users, transactions
- client/wallet definition

Private Gold-Back Currencies

Many private gold-backed cryptocoins were released in 2018. Most were based on Ethereum but several blockchains have been released since then - Solana, Avalanche, Matic, and Cardano. Private blockchains are probably a better option but we can gain insight from these attempts.

Ethereum is probably adequate but not optimal.

Currency	Blockchain	Status
OneGram	Graphene, C++, probably custom written	last tweet was 2019
Digix Gold Tokens	Ethereum	Digix ceased operations 21 March 2023
Gold Bits Coin	Ethereum	last news was 2019
Goldmint	based on the original pBFT protocol	last news was Aug, 2022
ZenGold	NA	last news was 2019
Puregold Token	Ethereum	last news was Feb 2020
HelloGold	Ethereum	shut down in Jan 2023
Xaurum	Ethereum	
PAXG	Ethereum	active
XAUT	Ethereum	Tether
PMGT	Ethereum	Active – Government mint
GLC	Ethereum	active

Perth Mint Gold Tokens

Perth Mint Gold Tokens are probably the closest equivalent to the gold-backed digital currency in this document. Perth Mint is government-owned, the tokens were running on the Ethereum blockchain until the blockchain host discontinued support for legal reasons.
This implementation should be a primary research item.

Existing Depository

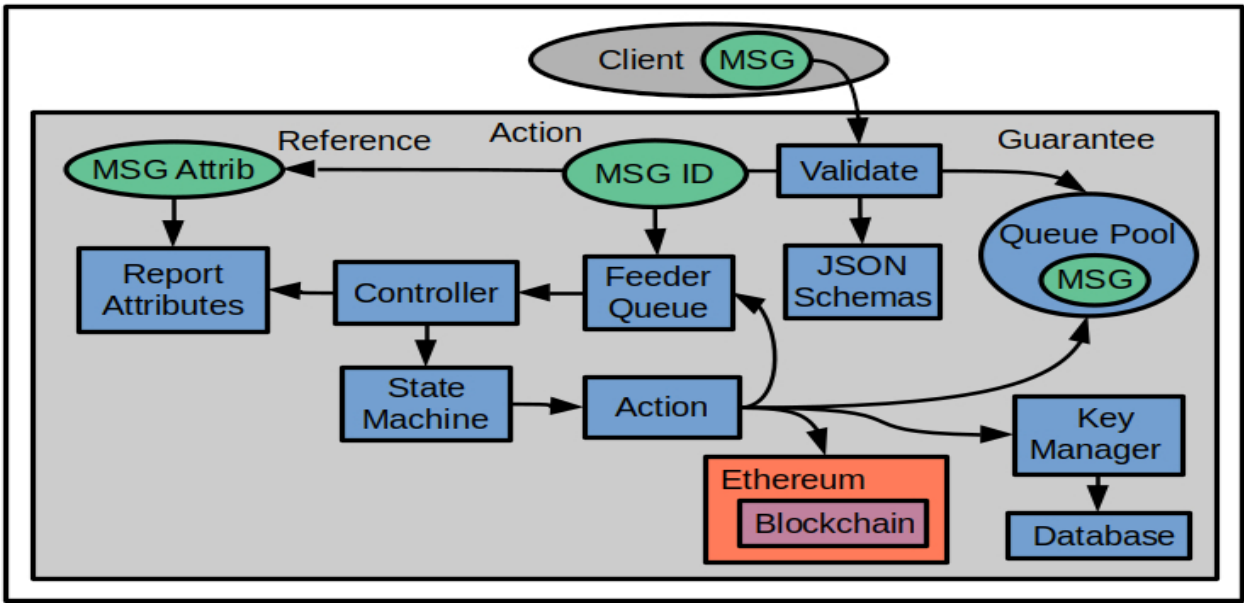
I have educated guesses as to what's inside the depository inventory system (although I'm trying to verify my guesses):

- traditional client-server app
- standard RDBMS for deposit entries
- no external API for remote entries
- no external API for verification of accounts
- security is mostly by physical location in depo
- has KYC validation
-

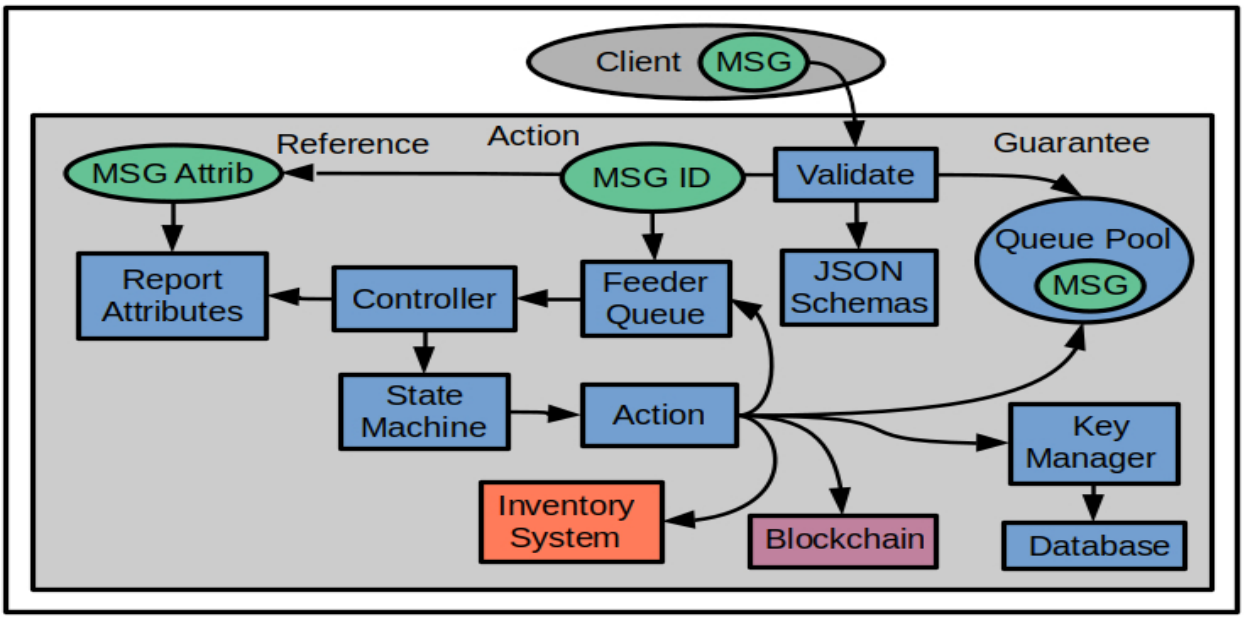
Ergo, integration with a digital currency would require modification of the inventory app. Probably significant work in security. A manual reconciliation process could be used for now for physical gold reallocation.

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.



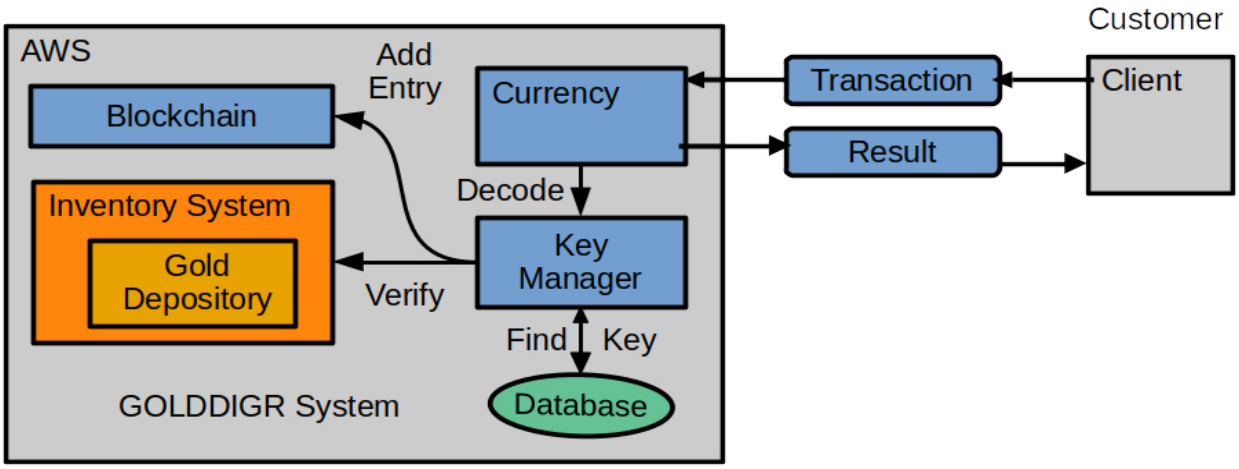
The proposal is to replace the Ethereum component with a separate blockchain and optional Gold Depository Inventory System. This design would be very similar.



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: The depository has an existing inventory system which synchronizes with the blockchain.

Here's a simple use case of transferring money:

1) Client sends a transaction to Currency API

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

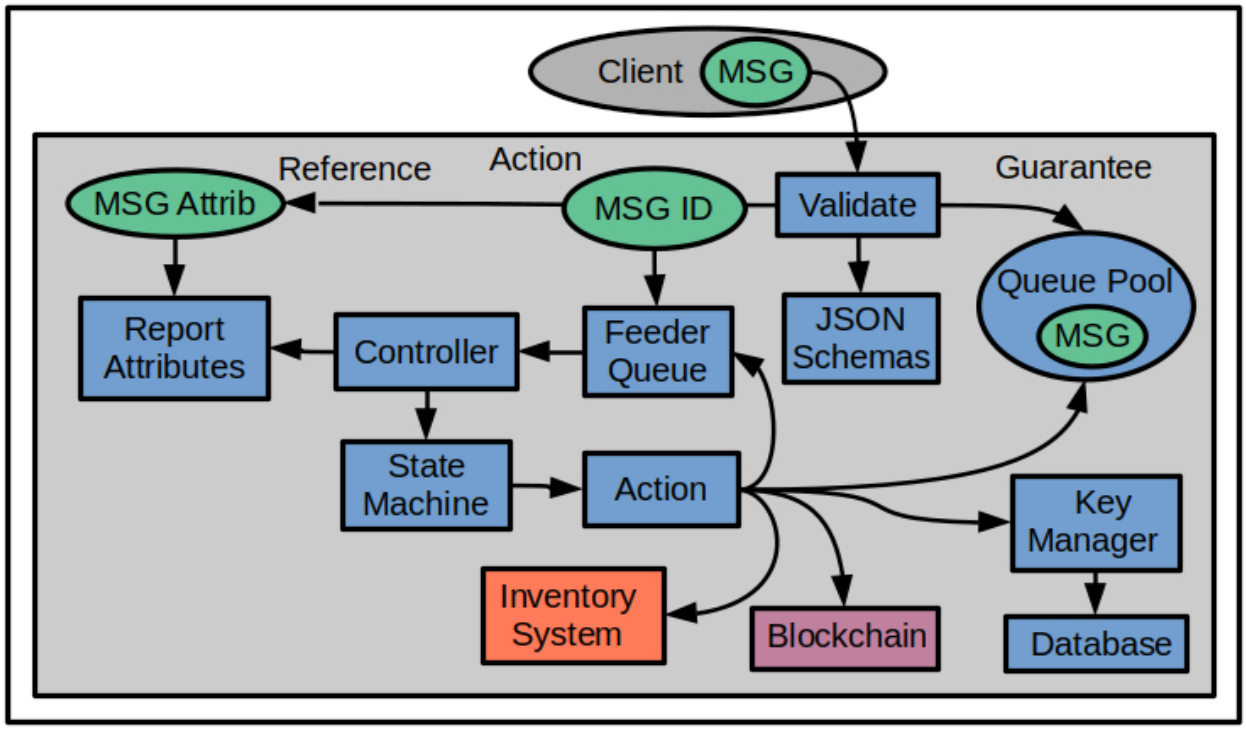
2) Currency forwards message to Key Manager.

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.

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. Add code functions to validate the remaining 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 Infrastructure (https://broward.ghost.io/aws_app_1/), tier management and deployment.

Messaging Strategy (https://broward.ghost.io/aws_app_2/)

Security considerations (https://broward.ghost.io/aws_app_9/) describes security on 2018Crypto project

Conclusion

Action Items

Research the depository inventory software and determine effort to add API integration with a blockchain

Research Perth Mint Gold Tokens as they are the closest political fit to this project. PMGT is being shut down so there may be lessons to be learned.

Private gold-backed currencies demonstrate that **Ethereum is an adequate choice but probably not optimal**. The private currencies used a public blockchain for credibility reasons but an existing State depository is already credible and most clients probably prefer their transactions stay private. Research into private blockchains is probably an action item.

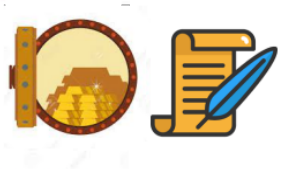
Research into multi-signature security for administrative access to the blockchain.

Identify strategic goals.

- Do we want cash equivalency?
- Should it support a Region vs a State?
- Estimate peak users and transactions
- Estimate purchase expectations - ($100-$10K?)

Estimate project timeline. I'm pretty sure a prototype can be built in four months by a team of five professionals because I created a similar MVP by myself in three months. A production release should be in the eight to twelve month range.

Author



Overview:

Thirty-four years of eclectic software development. Hands-on experience in over 30 IT projects, including seven startups, IT staff at a major university, USDOT grants and 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, worked directly with State employees and achieved adoption in 40 States..

In 1994, I was Boise State University employee of the year and received a commendation from the US Secretary of Transportation In 1995.

Digital Currencies

Hands-on work with three currencies - the Digital Money Trust in 1994 (a precursor to Bitcoin), Jing, 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 (insurance), 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.

Related Materal 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)
Bitcoin 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)