Applications of invariants in decentralized financial networks

Dr. David Chubelaschwili

November 5, 2024

Abstract

The following notes are in work and progress. We give hints how invariants lead to decentralised applications (Daaps) and provide a more fair destribution of income and risks in exchange of fungible assets.

I. Finacial networks

In 1705 the scottish economist John Law presented the concept of paper money as medium of exchange and store of value. Since then both autocracies and democracies govern its population with a central banking system. Allocation and distribution of money in central bank systems are mainly regulated by lending rates and print mechanisms respectively, to incentivise growth, prosperity and for adjustments of externalities. In the recent years a number of new international financial protocols arised in addition to our traditional monetary system leaving room for scepticism and douts for their necessities. The BRICS netwok, an alternative to the SWIFT system, gains popularity for new countries to join, to circumvent sanctions and increase economic potentials with nations that share commen social and cultural values. Financial networks like Bitcoin, Ethereum, Cardano or Solana base on the blockchain technology. Blockchain offers numerous advantages over the SWIFT or BRICS system, particularly in terms of speed, cost, security, and decentralization. While SWIFT remains the dominant player in the global financial messaging space, blockchain's disruptive potential lies in its ability to offer faster, cheaper, and more secure cross-border payments, along with enabling new financial services through automation (e.g., smart contracts) and provides transparancy, censorship resistance, availability, immutability and global reach.

II. Automated Market Maker

Automated market maker are rare and rethink the units of exchange, impact the profit distribution in currency markets and reduce the addictive user behaivior on centralized exchanges (Cex's).

Automated maket maker (AMM) are applicable for fungible assets. In economics, fungibility is the property of a good or a commodity whose individual units are essentially interchangeable, and each of whose parts are indistinguishable from any other part. Examples for fungible goods are electricity, sweet crude oil, company shares, bonds, precious metals and currencies. Apples for example are not fungible, since any two apples have a different taste and could be valued differently. It turns out that apples can not be pooled in a decentralized fashion, since a central authority is required for quality checks.

We discuss the construction of balancer pools. A new design to balance a portfolio, an innovative application in Defi.

We look at a portfolio with n assets $A_1, \ldots, A_n$ and assign balances $x := (x_1, \ldots, x_n)$ and weights $w := (w_1, \ldots, w_n)$. The following example illustrates a portfolio with equal weights but different balances in each asset. Let dxi and dxj be the units of assets Ai and Aj. For equal weights we obtain a partial differential equation $xjdxi = xidxj$

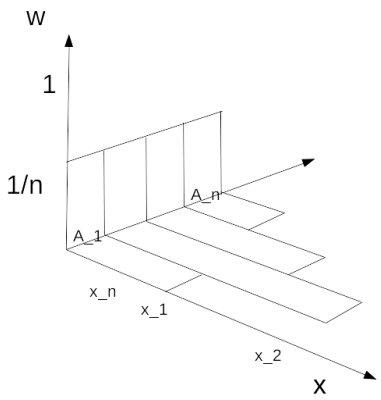

Figure 1: *Pools with equal weights*

implying a store of value $xixj$ and therefor an invariant

$$E = x1 \dots xn$$

for the whole portfolio. For portfolios with an arbitrary distribution w we obtain $(xj/wj)dxi = (xi/wi)dxj$, or $(wi/xi)dxi = (wj/xj)dxj$ implying a store of value

$$wilogxi = wjlogxj$$

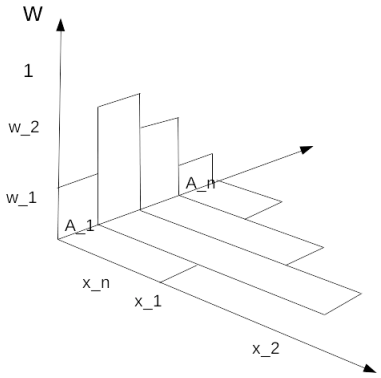

Figure 2: *Pools with arbritarry weights*

with the portfolio invariant

$$E(x, w) := x^w,$$

enables liquidity providers to re balance their portfolios and participate with fees rather just buy and hold.

Sharing values among strangers is not a common habit in our society. We stay mostly unaware about values like knowledge, energy, fungible assets keeping to ourselves at a permanent loss. Invariants of liquidity pools provide the awareness and economic incentives for sharing them. The construction of invariants require a fundamental understanding for the transformation of units. Invariant functions allow to compare different perspectives of observer. We discuss now that fungible assets are not necessary for achieving a collective agreement on a value. For example time and space are observer dependent and non fungible assets that can be transformed by light to a unit of a currency.

III. Lorenz invariant for space time agreements

The following section we investigate a hypothesis that reflects a fundamental relation between quantenties of time, space, light and money. We envision a new mining algorithm for a crypto currency. We extend the Byzantine general problem, a classical consensus protocol in distributed systems, from a binary decision outcome to a multivalued function, the Lorenz invariant. The underlying algorithm generalize ride pooling algorithms for vehicles to objects that move close to the speed of light. A decentralized economic model to value space time agreements. We consider two points A and B in vacuum beeing in relative rest according an inertial frame of reference. In vacuum the speed of light is constant and independent of the source of measurement. We explain a payment mechanism. Slow paths appear often and fast one appear seldom. Tangents at points along a hyperbola

$$c^2T^2 - S^2 = (A - B)^2$$

describe the density distribution. User requests with a necessity to transfer from A to B compare trajectories to the path of light and initiate two inertial frames of reference.

Theorem (Space Time Swap)**.** *A space time swap*

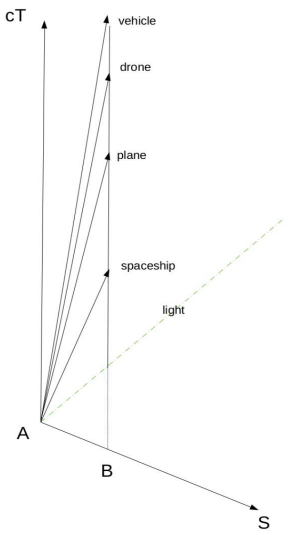

Figure 3: *Movements in vacuum*

is a transition change from (cT, S) to $(c\hat{T}, \hat{S})$ for points $c\hat{T}$ on a hyperbola. A price derives implictitly and is determend by the magnitude of the tangent. Prices for trajectories close to the spee of light go to infinity, while paths in rest relative to A and B are for free.

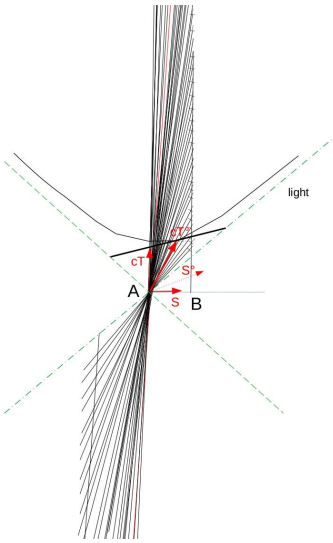

Figure 4: *Slow space time swap.*

- The ralativity of Time and Space in terms of the Byzantine general problem
- Spacemeshs proof of space time (PoST)

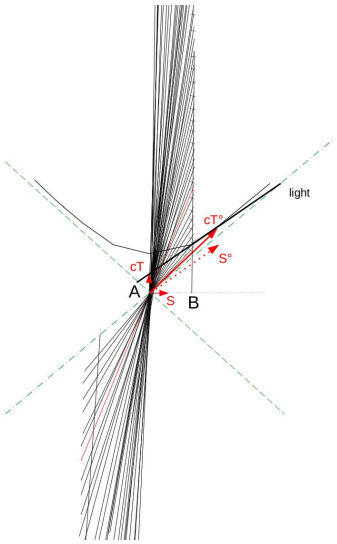

Figure 5: *Fast space time swap.*

References

[John Law, 1705] Money and trade considered: With a proposal for supplying the nation with money.

[S. Nakamoto, 2009] A Peer-to-Peer Electronic Cash System.

[T. Moran, I. Orlov, 2019] Simple Proofs of Space-Time and Rational Proofs of Storage

[L. Lamport, R. Shostak, M. Peace, 1982] The Byzantine Generals Problem

[L. Lamport, 1978] Time, Clocks, and the Ordering of Events in a Distributed System

[E. Fromm, 1976] Haben oder Sein

[A. Einstein, 1905] Zur Elektrodynamik bewegter Körper

[S. Wolfram, 2015] Computation equvivalence