Zero-Knowledge Optimal Monetary Policy under Stochastic Dominance

David Cerezo Sánchez
david@calctopia.com

12th October 2022

Abstract

Optimal simple rules for the monetary policy of the first stochastically dominant crypto-currency are derived in a Dynamic Stochastic General Equilibrium (DSGE) model, in order to provide optimal responses to changes in inflation, output, and other sources of uncertainty.

The optimal monetary policy [1] stochastically dominates all the previous crypto-currencies, thus the efficient portfolio is to go long on the stochastically dominant crypto-currency: a strategy-proof arbitrage featuring a higher Omega ratio with higher expected returns, inducing an investment-efficient Nash equilibrium over the crypto-market.

Zero-knowledge proofs of the monetary policy are committed on the blockchain: an implementation is provided.

Keywords: optimal monetary policy, optimal simple rules, stochastic dominance, stochastic calculus, DSGE model, strategy-proof, Nash equilibrium, zero-knowledge, crypto-currency

JEL classification: C11, C54, D58, D81, E42, E47, E52, E61, G11

[1] **STATEMENT ON MONETARY POLICY GOALS AND STRATEGY**:

The primary mandate is (stochastic) dominance.
The primary means of adjusting the policy stance is through changes in money growth.
The monetary policy is implemented with pre-committed policy rules, only to be revised in case of technology shocks or in the event of a financial crisis: the stance of monetary policy will adjust as appropriate if risks emerge that could impede the attainment of its goals, and this document will be reviewed and updated with any changes.
Unlike other crypto-currencies, this monetary policy synchronises with macro-economic observables, other fiat currencies and CBDCs: its primary goal is to follow cooperative equilibria, falling back to non-cooperative equilibria as last resort.

Contents

1 Introduction

One of the notorious deficiencies of crypto-currencies is their lack of monetary policy, as currently defined and studied in the field of macroeconomics: nonetheless, monetary crypto-policymakers must act in an optimal manner. In this paper, we initiate the study of optimal monetary policies for crypto-currencies in order to derive optimal simple rules that stochastically dominate the monetary policy of other previous crypto-currencies, and ultimately, prove that the efficient portfolio is to go long on the stochastically dominant crypto-currency.

1.1 Contributions

In summary, we make the following contributions:

- pioneer the introduction of the first optimal monetary policy for crypto-currencies
- devise the first stochastically dominant crypto-currency, its dominance arising from its optimal monetary policy
- derive optimal simple rules for a crypto-currency in a Dynamic Stochastic General Equilibria model
- prove that the efficient portfolio is to go long on stochastically dominant crypto-currencies: in fact, it's a strategy-proof arbitrage featuring a higher Omega ratio with a higher expected return, inducing a Nash equilibrium over the crypto-currency market
- describe how zero-knowledge proofs for the implemented monetary policy are committed on the blockchain

In a nutshell, we contribute a new methodology for analysing and deriving optimal simple rules for the monetary policy of stochastically dominant crypto-currencies, in order to create efficient portfolios of stochastically dominant crypto-currencies. This paper intends to be a self-contained guide covering all the necessary theory and practical aspects.

In section 2, we discuss related literature and prior work. In section 3, we introduce our economic environment, analysis framework, and efficient portfolio. In section 4, we describe our economic model and optimal monetary policies. Finally, we detail some features of the technical implementation in section 5, including how to commit the implemented zero-knowledge policy, and then we conclude in section 6.

The reader interested in less theoretic and most empirical analysis may skip to subsection 4.2,

2 Related Literature

The seminal contribution of this paper is to start the study of the first optimal monetary policy for crypto-currencies: until now, all the study of the field

was concentrated on the monetary policies for stablecoins [MIOT19, Cer19a] or the models of the interaction between crypto-currencies, fiat currencies and/or CBDCs with a view of understanding their shocks to the economy (starting from the seminal [BK16]).

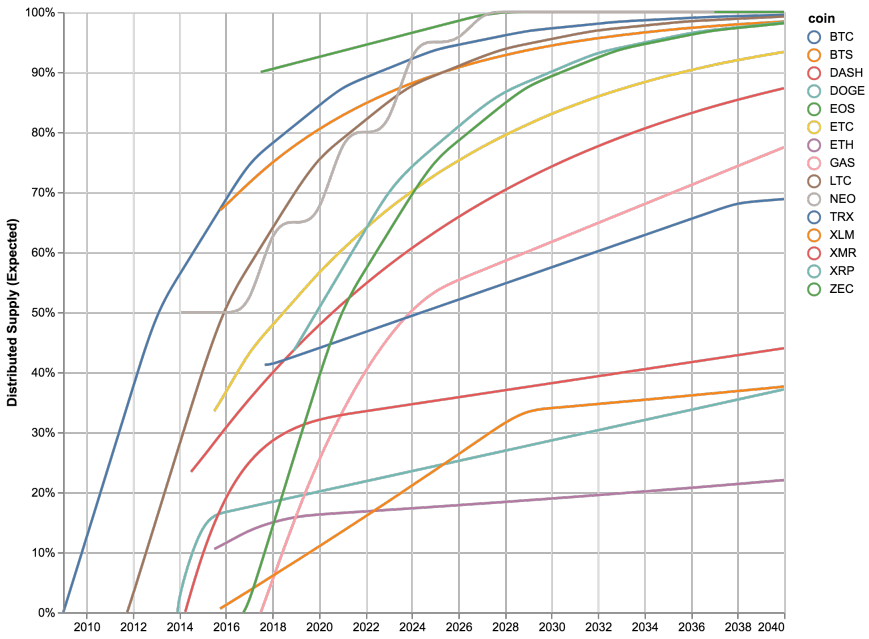

Figure 2.1: Relative supply of crypto-currencies[Gal19]

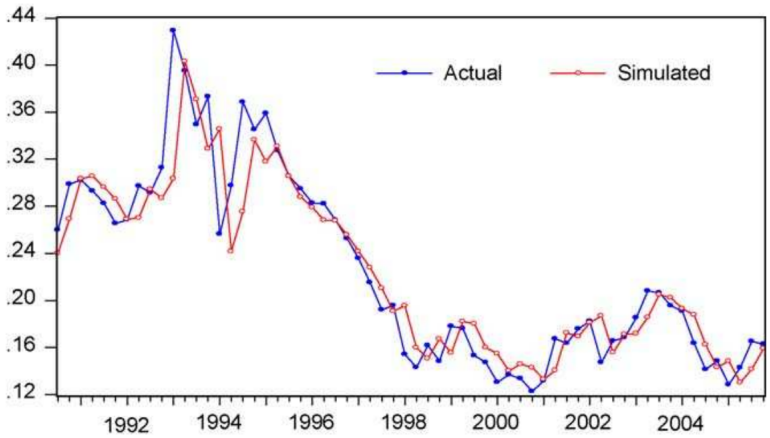

Figure 2.2: China's simulated quantity rule and actual M2 growth [LZ09]

However, the study of the monetary policy of crypto-currencies has always been relegated to matters related to their supply [Gal19], as shown in the previous Figure 2.1, in stark contrast with the quantity rules of money used in the real world (e.g., China's policy rule as shown in the previous Figure 2.2). In fact, the equational expression of both policy rules couldn't be more different: Bitcoin's supply equation S_t in period t can be given by

$$S_t^{BTC} = 21 \times 10^7 \times \left(1 - \alpha^t\right)$$

where α is the growth rate ($\alpha \approx 0.825$ for yearly periods and $\alpha \approx 0.953$ for quarterly periods, see 4.5), and China's quantity rule of money [LZ09] for the previous Figure 2.2 can be given by

$$\Delta M_t = \Delta M_t^* + \theta_1 \Delta M_{t-1} - \theta_2 \hat{Y}_t - \theta_3 \left(\pi_t - \pi_t^*\right)$$

with ΔM denoting the nominal money growth, ΔM_t^* the log of equilibrium money growth, $\theta_1 = 0.88$ the lag of nominal money growth, $\hat{Y}_t$ the output gap, $\theta_2 = 0.16$ the coefficient of response to changes of the output gap, π_t the inflation rate in period t, π_t^* the target inflation rate, and $\theta_3 = 0.06$ the coefficient of response to changes in inflation.

There is no related literature about what should be the optimal monetary policy of a crypto-currency according to the methods of modern macro-economics, as customarily practised on central banks: in fact, current crypto-currencies are designed for *anarcho-autarkic* settings on which they don't have to keep track of inflation, GDP, or money growth, not even the exchange rate of other crypto-currencies.

Moreover, previous sources of dominance in the crypto-currency market were the first mover advantage of Bitcoin, or the network effects inherent to payment networks [HG16] : as a novel contribution, this paper introduces optimal monetary policies as a source of dominance in the crypto-currency market.

Furthermore, simple rules are preferred over complex models [FV20]: in the foreseeable future, simple rules will still dominate the design of markets over complex models due to their many strengths and few weaknesses [Tay20].

2.1 Comparison with prior work

Previous work from the same author [Cer19a] described methods to conduct the monetary policy in a decentralised fashion, but with the following differences:

1. Previous work [Cer19a] focused on a stablecoin, but this paper targets the volatile crypto-currency market.
   (a) However, this paper introduces the novelty of *stochastic dominance* of monetary policy rules and its usefulness to dominate other previous crypto-currencies.
2. The technical implementation of this paper is significantly simpler than [Cer19a], without compromising the security model: that is, it provides similar cryptographic guarantees on a decentralised blockchain.

Additionally, the results of this paper are also valid for the setting of [Cer19a] : the optimal simple policy rules obtained in this paper (3.2.2 and 4.2) could be directly incorporated into the "Economic Model for a Central-Banked Currency" (Section 4.3 of [Cer19a]).

2.2 Survey of the Monetary Policy Impact on Crypto-currencies

Although crypto-currencies such as Bitcoin were designed to replace the discretionary decisions of monetary policymakers from central banks, even to insulate them from macro-economic shocks, in reality their decisions continue impacting their price and volatility. In this subsection, a survey of recent research about this topic is presented, which shall inform the design of monetary policy rules in the next subsection (4.2):

Paper	Period	Results
[Hsi21]	2010-2020	Unanticipated 1 bp on 2-year Treasury yield is about a 0.25% decrease in Bitcoin price and 1.23% three days later (stronger at high and low quantiles)
[Kar21]	2014-2021	Disinflationary ECB policy shocks (2-year interest rates of 10 basis points) lead to a persistent decrease in Bitcoin price (-20%), whereas inflationary ECB information shocks lead to price increases; conversely, contractionary US policy shocks (2-year interest rates of 10 basis point) increase Bitcoin prices (+7%) but fall during expansionary US information shocks (due to flows to foreign exchanges with emerging market currencies)
[PF21]	2016-2021	Cointegration between Bitcoin prices and M2, deeper with time delays
[CS20]	2010-2018	SVAR model shows no response of Bitcoin prices to shocks to nominal interest rate (1-year US treasury rate), only to stocks, VIX; but increase after a positive shock to the price level (Billion prices index)
[CLL$^+$17]	2013-2017	Mineable crypto-currencies show US volatility spillovers during FOMC announcement period, but not dApp or protocols
[PL19]	2010-2018	Bitcoin price increases 0.26% at no FOMC announcement, 0.96% on the day before and decreases 1% on the announcement day. Bitcoin price doesn't change on CPI, PPI or employment rate announcements
[CMC21]	2010-2021	Positive link between cryptocurrencies and forward inflation rates is identified only during COVID-19
[CS21]	2010-2020	Bitcoin prices appreciate against inflation (or inflation expectation) shocks, but do not decrease after policy (1-year US treasury rate) uncertainty shocks (i.e., only when excluding ZLB constraint)
[BGW21]	2019-2020	Daily changes in Bitcoin prices Granger cause changes in the forward inflation rate in a significant and persistent way, but not vice-versa
[BGW14]	2010-2014	In the short term, Bitcoin price adjusts to changes in money supply, GDP, inflation, and interest rate

Table 1: Survey of Monetary Policy Impact on Crypto-currencies

A practical example of the effects of inflation on Bitcoin price can be found below, shedding $1K on 13/9/2022 in just 3 minutes (10% of market capitalization) as US CPI inflation for August overshoots at 8.3% year-on–year (expected 8.1%):

Figure 2.3: Effect of inflation on BTC/USD

3 Environment, Framework and Efficient Portfolio

We consider pre-commitment rules in rational expectations models by a Bayesian risk-averse policymaker that is given the task to choose a policy feedback coefficient function mapping the parameter space into the set of policy feedback coefficients interpreted as random variables with probability distributions given from the posterior distributions of the model parameters, in order to minimise the expected disutilities of welfare loss for all disutility functions by ranking the policy rules according to a stochastic dominance criterion that is robust against all of the parameter uncertainty about the structure of the economic model.

3.1 Economic Environment

The setting of this paper is the general form of linear rational expectations models with uncertainty as set out in [And08]: many Dynamic Stochastic General Equilibrium models can be approximated by linear rational expectation (LRE) equations,

$$F_1(\theta_1,\theta_2)\,\mathbb{E}_t x_{t+1} + F_1(\theta_1,\theta_2)\,\mathbb{E}_t x_{t+1} + F_2(\theta_1,\theta_2)\,\mathbb{E}_t u_{t+1} + F_3(\theta_1,\theta_2)\,x_t + F_4(\theta_1,\theta_2)\,u_t + F(\theta_1,\theta_2)\,v_t = 0, \quad (3.1)$$

$$G_2(\phi)\,\mathbb{E}_t x_{t+1} + G_3(\phi)\,x_t + G(\phi)\,v_t = G_1(\phi)\,u_t, \tag{3.2}$$

$$M_1(\theta_m)\,x_t + M_2(\theta_m)\,u_t + M(\theta_m)\,v_{m,t} = y_t, t = 0, 1, 2, \ldots \tag{3.3}$$

with the equation 3.1 describing the dynamics of the private sector around the deterministic steady-state, 3.2 being the policy equation, and 3.3 the measurement equations, all the above using the following notation:

- x_t is a vector of n non-policy endogenous variables
- u_t a vector of k policy variables
- y_t a vector of $m \leq n + k$ observable variables
- $\mathbb{E}_t$ is the operator of conditional expectation with respect to an information set in period t
- F_i, F, G_i, G, M_i, and M are matrices depending on the parameters
- $v_{m,t}$ and v_t are vectors of independent and identically distributed innovations with zero mean and identity variance-covariance matrix I
- θ_1 is a vector of structural non-policy random parameters
- θ_2 is a vector of structural non-policy calibrated parameters
- θ_m is a vector of measurement parameters
- ϕ is a vector of random policy parameters (feedback or response coefficients)

The solution to the system of linear rational expectation equations 3.1 - 3.2 is given by a state equation of the form

$$z_t = A(\theta_s, \phi)\,z_{t-1} + B(\theta_s, \phi)\,v_t, \quad t = 1, 2, \ldots, \tag{3.4}$$

for the initial vector of states variables $z_0 = \left[x_0^{'}, u_0\right]^{'}$ and for unknown matrices $A(\theta_s, \phi)$, $B(\theta_s, \phi)$ with $\theta_s = \left[\theta_1^{'}, \theta_2^{'}\right]^{'}$.

The parameter uncertainty in model 3.3 - 3.4 is measured by the posterior probability distribution function according to the following Bayes rule:

$$p(\theta, \phi|Y_t) = \frac{p(\theta, \phi)\,p(Y_t|\theta, \phi)}{p(Y_t)}, \tag{3.5}$$

where $\theta = \left[\theta_s, \theta_m^{'}\right]^{'}$, $Y_t = \left[y_1^{'}, y_2^{'}, \ldots, y_t^{'}\right]^{'}$ is a sequence of observable vectors at time t, $p(Y_t|\theta, \phi)$ is a likelihood function, and $p(\theta, \phi) = p(\theta)\,p(\phi)$ is a prior posterior probability distribution function. The elements of $A(\theta_s, \phi)$, and $B(\theta_s, \phi)$are usually non-linear functions of the vectors θ_s and ϕ, and the

posteriors are not analytically available so we use the likelihood principle to treat posteriors as a measure of uncertainty about the parameters; thus, simulations are used to find approximations to the marginal posterior distributions θ and ϕ.

With this approach, optimal policy coefficients are assumed to be random variables with probability distributions inherited from the posterior distributions of the structural model parameters observed with parameter uncertainty, avoiding treating optimal feedback coefficients as fixed numbers much like policymakers usually do.

3.2 Decision Framework

In this subsection, we use a decision procedure to evaluate and rank simple policy rules in rational expectation models. A Bayesian policymaker formulates a statistical decision problem to choose a policy rule under parameter uncertainty with the following tuple

$$\left(Y_t, p\left(\theta\right), p\left(\phi_l\right), \Theta, D, M, L_t\right)$$

in which each term defines:

- Y_t denotes the history of the observable variables over t periods
- subjective prior distributions $p\left(\theta\right)$ for the structural parameters $\theta = \left[\theta_s^{'}, \theta_m^{'}\right]^{'} \in \Theta = \Theta_s \times \Theta_m$
- subjective prior distributions $p\left(\phi_l\right)$for the policy parameters $\phi_l \in \Phi_l$ for $l = 1, 2, \ldots, N$
- a set D of actions
- a set $M = \left\{P_{z|\theta_s,d} : \theta_s \in \Theta_s, d \in D\right\}$ of linear rational expectations models under consideration, differing in the values of the structural parameters $\theta_s \in \Theta_s$ and the values of the policymaker's action $d \in D$
- loss function $L_t\left(\theta, d\right)$ that quantifies the policymaker's choice of applying a given policy rule when a particular model holds

Considering how to rank a set of policy rules in the model of 3.2 with $N \geq 2$ different functional forms

$$G_{1l}\left(\phi_l\right) u_{l,t} = G_{2l}\left(\phi_l\right) \mathbb{E}_t x_{t+1} + G_{3l}\left(\phi_l\right) x_t + G_l\left(\phi_l\right) v_t, \quad t = 0, 1, 2, \ldots \tag{3.6}$$

with $l = 1, 2, \ldots, N$, the vector $\phi_l \in \Phi_l$ collecting the policy feedback coefficients, with G_{il} and G_l being matrices that depend on the policy feedback parameters.

The decision space D is of the form

$$D = \{(l, f_l) : l = 1, 2, \ldots, N \tag{3.7}$$

$$f_l : \Theta \to \Phi_l\} \tag{3.8}$$

in which the following conditions hold:

- the admissible policies $d = (l, f_l)$ is a rule from 3.6
- $f_l : \Theta \to \Phi_l$ is a policy feedback coefficient from a given class of measurable functions F_l such that the system of linear rational expectation equations 3.1 and 3.6, with $\phi_l = f_l(\theta)$ for all $\theta \in \Theta$ has a solution which is given by the state equation

$$z_{l,t} = A_l(\theta_s, \phi_l) z_{l,t-1} + B_l(\theta_s, \phi_l) v_t, \quad t \geq 1 \tag{3.9}$$

  with z_0 being an initial state, $z_{l,t} = \left[x_t^{'}, u_{l,t}^{'}\right]^{'}$, $z_{l,0} = z_0$, and $A_l(\theta_s, \phi_l), B_l(\theta_s, \phi_l)$ are unknown matrices with $\theta_s = \left[\theta_1^{'}, \theta_2^{'}\right]^{'}$
- every set F_l includes all constant functions $f_l(\theta) = \text{const}$
- the parameters space Φ_l consists of all vectors of policy parameters ϕ_l for every $l = 1, 2, \ldots$ such that for all $\theta_s \in \Theta_s$, the system of linear rational expectation equations 3.1 and 3.6 has a unique solution

The procedure of the Bayesian policymaker is to first observe the history of the observable variables Y_t over t periods, and for every $l = 1, 2, \ldots, N$ sets the subjective prior distributions $p(\theta)$ of the structural parameters and $p(\phi_l)$ of the policy parameters $\phi_l \in \Phi_l$. Then, it analyses the following set of linear rational expectation models,

$$M = \left\{P_{z|\theta_s,d} : \theta_s \in \Phi_s, d \in D\right\}$$

for endogenous non-policy x_t described by 3.1 and policy variables $u_{l,t}$ described by 3.6. The predictive probability distribution $P_{z|\theta_s,d}$ of the future state variables $z = (z_{l,t+s})_{s=0,1,2,\ldots} \in \mathbb{Z}$ evolves according to 3.9.

3.2.1 Welfare Loss Function

The welfare loss function of the Bayesian decision maker's objective at time t is defined by

$$L_t : Z_t \times V \times \Theta \times D \to [0, \infty)$$

receiving the following parameters:

- a vector of current state variables $z_t \in Z_t$
- all future shocks $v = \{(v_{t+s}, v_{m,t+s})\}_{s=1,2,\ldots} \in V$
- all vectors of structural parameters θ from the parameter space Θ
- all admissible decisions d from the decision space D

In order to evaluate the objective function, the Bayesian policymaker could take the unconditional average of the welfare losses over the current state and all possible future shocks:

$$L_t(\theta, d) = \int_{Z_t} \int_V L_t(z_t, v, \theta, d)\, dP_v(v)\, dP_{z_t}(z_t) \tag{3.10}$$

or the conditional expected value of the welfare loss given z_t:

$$L_t(\theta, d|z_t) = \int_V L_t(z_t, v, \theta, d)\, dP_v(v) \tag{3.11}$$

with $\theta = \left[\theta_s', \theta_m'\right]' \in \Theta$ and the policymaker decision $d \in D$ that is able to modify the model structure $P_{z|\theta_s,d}$, the posterior distribution of the structural parameters $P_{\theta|Y_t,d}$, and the value of the expected welfare loss $L_t(\theta, d)$.

In this paper, we will use a quadratic welfare loss function given by:

$$L_t(\theta, d) = \operatorname{tr}\left(W \sum_{z_l} (\theta_s, d)\right) = \operatorname{var}_{\theta_s,d}(\hat{\pi}_t) + w_y \operatorname{var}_{\theta_s,d}(\hat{y}_t) \tag{3.12}$$

for all $d = (l, f_l) \in D$ and $\theta_s \in \Theta_s$ where $\operatorname{var}_{\theta,d}(z_{l,t,i})$ is the unconditional variance of the state variable $z_{l,t,i}$ in the l-th specification of the DSGE model, while w_y is the diagonal weight of W for the output gap. These diagonal weights reflect the monetary policy preferences of the central bank over the objectives: specifically, we set $w_y = 0.05$ and $w_\pi = 1$.

3.2.2 Ranking Simple Policy Rules

Now we can start formulating robust optimality criteria to generate rankings of simple policy rules 3.6 based on the optimal Bayesian policymaker's objective function L_t: first, a fixed vector of structural parameters $\hat{\theta} \in \Theta$ is chosen from the parameter space Θ, and then the expected welfare loss $L_t\left(\hat{\theta}, d\right)$ is minimised subject to the recursive state equations 3.9 under criteria of k-degree stochastic dominance (SDk) [Lev16]. Stochastic dominance is a useful concept for analysing risky decision-making under uncertainty when only partial information about the decision maker's risk preferences is available.

Definition 1. (SDk ordering) . Defined by the indefinitely many inequalities

$$\int_0^{L^*} u(x)\, dF_{L_1}(x) \leq \int_0^{L^*} u(x)\, dF_{L_2}(x) \tag{3.13}$$

between the expected disutilities of non-negative valued random losses $L_1 \leq_{\mathrm{SD}k} L_2$ with the cumulative distribution functions $L_1 \sim F_{L_2}$ and $L_2 \sim F_{L_2}$, for all functions $u \in U_k$ with strict inequality for some u, where U_k is the set of all disutility functions with the i-th derivative of u such that $u' \geq 0$, $u'' \geq 0, \ldots, u^{(k)} \geq 0$. Note that SD$k$ implies SDl for all $k > l$, and that the SD∞

dominance of L_2 over L_1 implies that $L_1 \leq_{\text{SD}k} L_2$ holds for some finite k. Additionally, we denote with $\leq_{\text{SD}k}$ the inequality between random welfare losses defined by the SDk ordering for $k = 1, 2, \ldots, \infty$. Recall that SD1 ordering assumes all non-decreasing disutility functions (non-satiable); SD2 is for risk-averse policymakers towards welfare losses, restricting the disutility functions to convex and non-decreasing; SD3 additionally prefers negatively skewed welfare loss distributions (prudence); and SD4 requires that $u^4 \leq 0$ (temperance).

Accordingly, simple policy rules can be analysed using the SDk ordering from the previous Definition 1.

Definition 2. (SDk-optimal policy) . Finding the best SDk-optimal simple policy under parameter uncertainty is solved by searching for the SDk-optimal decision $d_1^{\text{SD}k} = \left(l_1^{\text{SD}k}, f_{l_1^{\text{SD}k}}\right) \in D$ from the set of all admissible decisions D such that the corresponding distribution of welfare loss $L_t\left(\cdot, d_1^{\text{SD}k}\right)$ satisfies

$$L_t\left(\cdot, d_1^{\text{SD}k}\right) \leq_{\text{SD}k} L_t\left(\cdot, d\right) \tag{3.14}$$

for all $d \in D$ and subject to 3.9: $d_1^{\text{SD}k}$ generates the distribution of minimised welfare loss, the smallest in terms of the SDk ordering.

Assume that the Bayesian policymaker solves a parameterised optimisation problem to find the value of the optimal policy feedback coefficient function $f_l^{\min}(\theta)$:

$$L_{l,t}^{\min}\ (\theta) = \min_{\phi_l \in \Phi_l} L_t\left(\theta, (l, \phi_l)\right) = L_t\left(\theta, \left(l, f^{\min}\ (\theta)\right)\right) \tag{3.15}$$

for each value of the structural parameters $\theta \in \Theta$ and for every policy specification $l = \{1, 2, \ldots, N\}$ given in 3.6. Note that $f_l^{\min}(\theta)$ is a selection from the optimal choice correspondence set:

$$f_l^{\min}(\theta) \in \Phi_l^{\min}\ (\theta) = \left\{\phi_l^{\min} \in \Phi_l : L_{l,t}^{\min}(\theta) = L_t\left(\theta, \left(l, \phi_l^{\min}\right)\right)\right\}$$

We define $\phi_l^{\min} = f_l^{\min}(\theta)$ to be the vector of optimal policy feedback coefficient of rule l calculated for the vector of structural parameters θ: thus, the optimal policy feedback coefficient function $f_l^{\min} : \Theta \to \Phi_l$ is measurable and the pair $\left(l, f_l^{\min}\right)$ belongs to D.

The uncertainty of the structural parameters is considered in order to find the probability distribution of the optimal policy response coefficients

$$\phi_l^{\min} \sim p_\theta\left(\left(f_l^{\min}\right)^{-1} | Y_t, l\right) \tag{3.16}$$

and the minimised welfare loss is given by

$$L_{l,t}^{\min} \sim p_\theta\left(\left(L_t \circ f_l^{\min}\right)^{-1} | Y_t, l\right) \tag{3.17}$$

where the inverse image of $A \in \mathcal{B}(\Phi)$ under $\theta \to f_l^{\min}(\theta)$ is

$$\left(f_l^{\min}\right)^{-1}(A) = \left\{\theta \in \Theta : f_l^{\min}(\theta) \in A\right\}$$

and the inverse image of $B \in \mathcal{B}(\Phi)$ under $\theta \to L_t\left(\theta, f_l^{\min}(\theta)\right)$ is

$$\left(L_t \circ f_l^{\min}\right)^{-1}(B) = \left\{\theta \in \Theta : L_t\left(\theta, f_l^{\min}(\theta)\right) \in B\right\}$$

Next theorem 3.18 gives sufficient conditions for the optimal solution to 3.14 and shows how the SDk-optimal decision can be found.

Theorem 3. *Assume that the decision sets Φ_l for $l = 1, 2, \ldots, N$ are non-empty compact subsets of $\mathbb{R}^r$, the parameter space Θ is an open subset of $\mathbb{R}^p$, and the policymaker's welfare loss L_t is a Carathéodory-type integrable function. If $d^* = (l^*, f_{l^*}) \in D$ is a policymaker decision such that l^* is defined by*

$$L_{l^*,t}^{min} \leq_{SDk} L_{l,t}^{min}, \quad \forall l \in \{1, 2, \ldots, N\} \tag{3.18}$$

where $L_{l,t}^{min}, l \in \{1, 2, \ldots, N\}$ are random minimised welfare losses as defined in 3.15, 3.16 and 3.17; and $f_{l^*} = f_{l^*}^{min}$ is the optimal policy feedback coefficient function that solves 3.15, as denoted by

$$\min_{\phi_{l^*} \in \Phi_{l^*}} L_t\left(\theta, (l^*, \phi_{l^*})\right) = L_t\left(\theta, (l^*, f_{l^*}(\theta))\right) = L_{l^*,t}^{min}(\theta), \quad \forall \theta \in \Theta \tag{3.19}$$

then $d^* = d_1^{SDk}$ is the SDk-optimal decision.

3.3 Efficient Portfolio

In this subsection, we derive an efficient portfolio for stochastically dominant crypto-currencies providing the best expected returns in comparison with the other crypto-currencies. Instead of using the mean-variance framework, we prefer to use marginal conditional stochastic dominance [SY84]: all risk-averse investors prefer a portfolio A over a portfolio B if the portfolio return of A is stochastically dominant over that of B, moving out all dominated assets. Furthermore, almost marginal conditional stochastic dominance [MJYW14] could be used to prevent extreme utility functions in the set of risk-averse investors.

3.3.1 Pricing Stochastic Dominance

In order to ease exposition, suppose there are only two crypto-currencies in two separate, segmented markets: a stochastically dominant crypto-currency, D, and Bitcoin, B (resp. any other PoW/PoS crypto-currency). Consumption in the dominant market at time t is denoted by c_t^D, and c_t^B in the Bitcoin denominated market (resp. any other PoW/PoS crypto-currency). Consumers can transact in one market but not both simultaneously, that is, utility $u_j\left(C_{j,t} \cdot ms_{j,t}\right)$ at time t in market $j \in \{D, B\}$, where $C_{j,t}$ denotes complete-market consumption that is distorted by the non-hedgeable monetary policy shock $ms_{j,t}$, rendering incomplete the system of markets: moreover, we assume that $ms_{j,t}$ and $C_{j,t}$ are statistically independent for any $j \in \{D, B\}$.

Lemma 4. *Suppose the utility function $u(x)$ is of the form Constant Relative Risk-Aversion (CRRA), then the Stochastic Discount Factor (SDF) in the dominant market is given by*

$$M_{t+1}^{D} = \left(\frac{ms_{D,t+1} C_{D,t+1}}{ms_{D,t} C_{D,t}} \right)^{-\gamma} = M_{t+1}^{C_D} M_{t+1}^{ms_D} \tag{3.20}$$

and in the Bitcoin market (resp. any other PoW/PoS crypto-currency) is given by

$$M_{t+1}^{B} = \left(\frac{ms_{B,t+1} C_{B,t+1}}{ms_{B,t} C_{B,t}} \right)^{-\gamma} = M_{t+1}^{C_B} M_{t+1}^{ms_B} \tag{3.21}$$

where γ is the coefficient of relative risk aversion, and

$$M_{t+1}^{C_j} = \left(\frac{C_{j,t+1}}{C_{j,t}} \right)^{-\gamma}, M_{t+1}^{ms_j} = \left(\frac{ms_{j,t+1}}{ms_{j,t}} \right)^{-\gamma}$$

Lemma 5. (Fundamental Pricing Equation). *The Euler equation for holders of the stochastically dominant crypto-currency is given by:*

$$E_t \left[M_{t+1}^{B} \frac{Q_{t+1}}{Q_t} \right] = E_t \left[M_{t+1}^{D} \frac{M_{t+1}^{ms_B}}{M_{t+1}^{ms_D}} \right] = \frac{1}{R_{t+1}^{D}} \tag{3.22}$$

and the Euler equation for the Bitcoin holder (resp. any other PoW/PoS crypto-currency) is given by:

$$E_t \left[M_{t+1}^{D} \frac{Q_{t+1}}{Q_t} \right] = E_t \left[M_{t+1}^{B} \frac{M_{t+1}^{ms_D}}{M_{t+1}^{ms_B}} \right] = \frac{1}{R_{t+1}^{B}} \tag{3.23}$$

where $Q_t$is the real exchange rate, and R_{t+1}^{D} and R_{t+1}^{B} are the risk-free rate in the dominant and Bitcoin market, respectively.

We assume that the logarithm of the Stochastic Discount Factors (SDFs) in the two markets are normally distributed: m^{D}, m^{B}, m^{ms_D}, m^{ms_B}, m^{C_D} and m^{C_B} (i.e., we denote logarithms of capitalised variables with their lowercase variant).

Lemma 6. *The arbitrage-free expected return on the stochastically-dominant crypto-currency is given by:*

$$E_t(\Delta q_{t+1}) = r_t^{B} - r_t^{D} + \frac{1}{2} \left[Var_t\left(m_{t+1}^{B}\right) - Var_t\left(m_{t+1}^{D}\right) \right] + E_t m_{t+1}^{ms_B} - E_t m_{t+1}^{ms_D} \tag{3.24}$$

thus a relative rise of $E_t m_{t+1}^{ms_B}$ over $E_t m_{t+1}^{ms_D}$ leads to the appreciation of the stochastically dominant crypto-currency.

Definition 7. (Logarithmic utility function). The utility function is

$$u(x) = \log(x)$$

thus we have the following additively separable representation for the two shocks, consumption and monetary (resp. cs and ms):

$$u(cs \cdot ms) = \log(cs \cdot ms) = u_1(cs) \cdot u_2(ms) = \log(cs) + \log(ms)$$

with values for D_1 and B_1 for u_1 and D_2 and B_2 for u_2: D_1 and $D_2$are marginals of the joint probability distribution $D(cs, ms)$ in the dominant market, while B_1 and B_2 are marginals of the joint probability distribution $B(cs, ms)$ in the Bitcoin market (resp. any other PoW/PoS crypto-currency).

Lemma 8. (First-order Stochastic Dominance). *A necessary and sufficient condition for the first-order stochastic dominance of the stochastically dominant crypto-currency over Bitcoin (resp. any other PoW/PoS crypto-currency) is*

$$B_1(cs) \geq D_1(cs)$$

and

$$B_2(cs) \geq D_2(cs)$$

with strong inequality for at least some values in cs or in ms.

Given the definitions 7, the stochastically dominant crypto-currency in the dominant market with a joint probability distribution $D(cs, ms)$, is preferred to the Bitcoin market with $B(cs, ms)$ if:

$$E_D u(cs, ms) - E_B u(cs, ms) \tag{3.25}$$

$$= \int (B_1(t) - D_1(t))\, du_1(t) + \int (B_2(s) - D_2(s))\, du_2(s) \tag{3.26}$$

$$= \int (B_1(t) - D_1(t))\, \frac{1}{t} du(t) + \int (B_2(s) - D_2(s))\, \frac{1}{s} du(s) \geq 0 \tag{3.27}$$

Lemma 9. (Second-order Stochastic Dominance). *A necessary and sufficient condition for the second-order stochastic dominance of the stochastically dominant crypto-currency over Bitcoin (resp. any other PoW/PoS crypto-currency)*

$$\int_t^\infty (B_1(s) - D_1(s))\, ds \geq 0$$

and

$$\int_t^\infty (B_2(s) - D_2(s))\, ds \geq 0$$

for all $s > t$ with at least one strict inequality.

We assume that the consumption shocks in the two markets, dominant and Bitcoin, are roughly the same,

$$D_1 \approx B_1$$

as both crypto-currencies are part of the same general economy (i.e., cs is rendered C as in its initial definition), thus monetary shocks play a pivotal role: users prefer the stochastically dominant crypto-currency given the projected expected utility of its stochastically dominant monetary policy, D_2, over Bitcoin's B_2 (resp. any other PoW/PoS crypto-currency).

Theorem 10. (Dominant Expected Returns). *A dominance relationship between the distribution of the monetary policy shock of the stochastically dominant crypto-currency, $ms_D(D_2)$, over Bitcoin, $ms_B(B_2)$, implies a rise $E_t(\Delta q_{t+1})$ 6 of the price of the stochastically dominant crypto-currency D in terms of Bitcoin (resp. any other PoW/PoS crypto-currency).*

Proof. When D_2 dominates B_2 in the first-order sense 8, then

$$E_t m_{t+1}^{ms_B} - E_t m_{t+1}^{ms_D} > 0$$

and vice versa. Thus,

$$\begin{aligned} E_t m_{t+1}^{ms_B} - E_t m_{t+1}^{ms_D} &= ms_{B,t} E_t\left(\frac{1}{ms_{B,t+1}}\right) - ms_{D,t} E_t\left(\frac{1}{ms_{D,t+1}}\right) \\ &= \int \frac{1}{t} dB_2(t) - \int \frac{1}{t} dD_2(t) \\ &= \int \frac{1}{t} d(B_2 - D_2) \\ &= \int (D_2 - B_2)\, d\frac{1}{t} \\ &= -\int (D_2 - B_2)\, \frac{1}{t^2} dt > 0 \end{aligned}$$

and the consequent rise of $E_t(\Delta q_{t+1})$ as given by 6. □

3.3.2 Efficient Stochastically Dominant Portfolio

The stochastic dominance between two crypto-currencies of 8 and 9 further extends into a stochastically dominant portfolio of crypto-currencies. As in previous sections, we can distinguish between different orders of portfolio dominance: first (Definition 11), second (Definition 13), ..., SDk-orders (Definition 15) of portfolio dominance. Note that recent empirical research corroborates that the inclusion of crypto-currencies in portfolios is itself stochastically dominant [HNP$^+$21, Rah20, MBN20, Coh21, TT18, AAT21].

Given N alternatives and a random vector of their outcomes ϱ, a decision maker can combine them into portfolios and all portfolio possibilities are denoted by

$$\Lambda = \left\{\lambda \in \mathbb{R}^N | 1'\lambda = 1, \quad \lambda_n \geq 0, \quad n = 1, 2, \ldots, N\right\}$$

Definition 11. Portfolio $\lambda \in \Lambda$ dominates portfolio $\tau \in \Lambda$ by the first-order stochastic dominance ($\varrho'\lambda \leq_{SD1} \varrho'\tau$) if

$$F_{\varrho'\lambda}(x) \leq_{SD1} F_{\varrho'\tau}(x), \quad \forall x \in \mathbb{R}$$

with strict inequality for at least one $x \in \mathbb{R}$ and with $F_{\varrho'\lambda}(x)$ denoting the cumulative probability distribution of returns of portfolio λ. Necessary and sufficient conditions for the first-order stochastic dominance ($\varrho'\lambda \leq_{SD1} \varrho'\tau$) if:

- $Eu\left(\varrho'\lambda\right) \geq Eu\left(\varrho'\tau\right)$ for all expected utility (Eu) functions and strict inequality holds for at least some utility function
- $F^{-1}_{\varrho'\lambda}\left(y\right) \leq F^{-1}_{\varrho'\tau}\left(y\right)$ for all $y \in [0,1]$ with strict inequality for at least one $y \in [0,1]$
- $VaR_{\alpha}\left(-\varrho'\lambda\right) \leq VaR_{\lambda}\left(-\varrho'\tau\right)$ for all $\alpha \in [0,1]$ with strict inequality for at least one $\alpha \in [0,1]$

Definition 12. A given portfolio $\tau \in \Lambda$ is first-order stochastic dominant (Definition 11) inefficient if there exists portfolio $\lambda \in \Lambda$ such that ϱ'$\lambda \leq_{SD1} \varrho$'$\lambda$. Otherwise, portfolio τ is first-order stochastic dominant efficient.

Second-order stochastic dominance can be similarly defined as first-order:

Definition 13. Portfolio $\lambda \in \Lambda$ dominates portfolio $\tau \in \Lambda$ by the second-order stochastic dominance $(\varrho'\lambda \leq_{SD2} \varrho'\tau)$ if and only if

$$F^{(2)}_{\varrho'\lambda}\left(y\right) \leq_{SD2} F^{(2)}_{\varrho'\tau}\left(y\right), \quad \forall y \in \mathbb{R}$$

with strict inequality for at least one $y \in \mathbb{R}$ and with $F^{(2)}_{\varrho'\lambda}\left(y\right)$ denoting the twice cumulative probability distribution of returns of portfolio λ. Necessary and sufficient conditions for the second-order stochastic dominance $(\varrho'\lambda \leq_{SD1} \varrho'\tau)$ if:

- $Eu\left(\varrho'\lambda\right) \geq Eu\left(\varrho'\tau\right)$ for all expected concave utility functions and strict inequality holds for at least some concave utility function
- Non-satiable and risk-averse decision maker prefers portfolio τ to portfolio λ and at least one prefers λ to τ
- $F^{-2}_{\varrho'\lambda}\left(y\right) \leq F^{-2}_{\varrho'\tau}\left(y\right)$ for all $y \in [0,1]$ with strict inequality for at least one $y \in [0,1]$, where $F^{-2}_{\varrho'\lambda}\left(y\right)$ is a cumulated quantile function
- $CVaR_{\alpha}\left(-\varrho'\lambda\right) \leq CVaR_{\lambda}\left(-\varrho'\tau\right)$ for all $\alpha \in [0,1]$ with strict inequality for at least one $\alpha \in [0,1]$, where

$$\begin{aligned} CVaR_{\alpha}\left(-r'\lambda\right) = & \min_{v \in \mathbb{R}, z_t \in \mathbb{R}^+} v + \frac{1}{1-\alpha}\sum_{t=1}^{S} p_t z_t \\ & \text{such that} z_t \geq -x^t\lambda - v, \quad t = 1, 2, \ldots, S \end{aligned}$$

Definition 14. A given portfolio $\tau \in \Lambda$ is second-order stochastic dominant (Definition 11) inefficient if there exists portfolio $\lambda \in \Lambda$ such that ϱ'$\lambda \leq_{SD2} \varrho$'$\lambda$. Otherwise, portfolio τ is second-order stochastic dominant efficient.

The previous two definitions, first-order and second-order, can be generalised to the k-order:

Definition 15. Portfolio λ dominates portfolio τ with respect to the k-order stochastic dominance ($\lambda \leq_{SDk} \tau$) if $Eu(\varrho'\lambda) \geq Eu(\varrho'\tau)$ for all utility functions $u \in U_n$ with strict inequality for at least one such utility function, with U_N being the set of N times differentiable utility functions such that: $(-1)^i u^{(i)} \leq 0$ for all $i = 1, 2, \ldots, N$.

Definition 16. A given portfolio τ is SDk-efficient ($k \geq 2$) if there exists at least one utility function $u \in U_N$ such that $Eu(\varrho'\tau) - Eu(\varrho'\lambda) \geq 0$ for all $\lambda \in \Lambda$ with strict inequality for at least one $\lambda \in \Lambda$.

And the previous one period stochastic dominance can be generalised to the multi-period setting:

Theorem 17. *([Lev73]). Let $F^n(x)$ and $G^n(x)$ be the cumulative distributions of two n-period risks where n is the number of periods and x is the product of the returns corresponding to each period ($x = x_1, x_2, \ldots, x_n$). Then, a sufficient condition for F^n dominance over G^n by first-order stochastic dominance for every non-decreasing utility function is that such dominance exists in each period, namely:*

$$F_i(x_i) \leq G_i(x_i), \quad \forall i, (i = 1, 2, \ldots, n)$$

and there is at least one strict inequality, namely:

$$F_i(x_{i_0}) < G_i(x_{i_0})$$

for some x_{i_0}.

Theorem 18. *([Lev73]). A sufficient condition for F^n dominance over G^n by second-order stochastic dominance for all non-decreasing concave utility functions is that such dominance exists in each period, namely:*

$$\int_0^{x_i} [G_i(t_i) - F_i(t_i)]\, dt_i \geq 0, \quad \forall i, (i = 1, 2, \ldots, n)$$

and there is at least one strict inequality.

Finally, note that the concept of stochastic dominance also extends to strategy-proof allocation rules and game strategies:

Definition 19. . A strategy s is *stochastic dominance strategy-proof* if, for all investors $i \in I$, all security ranking profiles $(R_i, R_{-i}) \in R^I$, and all misreports $R_i^{'} \in R$, investor i's assignment $x_{i,j} \in s_i(R_i, R_{-i})$ *stochastically dominates* $y_{i,j} \in s_i\left(R_i^{'}, R_{-i}\right)$ at R_i (i.e., independent of the other investors' ranking reports), that is,

$$\sum_{s_i(R_i, R_{-i})} x_{i,j} \geq \sum_{s_i\left(R_i^{'}, R_{-i}\right)} y_{i,j}$$

Alternatively, *stochastic dominance strategy-proof* can also be defined in terms of expected utility if, for all utility functions $u_i \in U_{R_i}$, we have that

$$Eu_{s_i(R_i,R_{-i})}(u_i) \geq Eu_{s_i\left(R_i',R_{-i}\right)}(u_i)$$

All the previous definitions naturally lead to the following theorem regarding the stochastically dominant crypto-currency:

Theorem 20. *The efficient portfolio is to go long on the stochastically dominant crypto-currency: thus, the stochastically dominant strategy-proof allocation rule for any investor is to hold this efficient portfolio with the stochastically dominant crypto-currency. Furthermore, a higher return can be expected from the stochastically-dominant crypto-currency.*

Proof. Given a stochastic ranking of policy rules 3.14 of a stochastic ordering (Definition 1) of monetary policy rules 3.6 that generates a stochastically dominant crypto-currency by first-order 8 or second-order 9 dominance: then, the SDk-efficient portfolio 16 (also, first-order 12 or second-order 14 efficient) that dominates with respect to the k-order stochastic dominance 15 (also, first-order 11 or second-order 13 dominant) is the portfolio containing the stochastically dominant crypto-currency as, by definition, this the one crypto-currency with the SDk-optimal policy rule 3.14 that SDk dominates (Definition 1) all the other policy rules. The proof extends trivially to the multi-period case by Theorems 17 and 18.

Moreover, for all investors $i \in I$, the stochastically dominant strategy-proof allocation rule 19 is to hold the SDk-efficient portfolio 16 with the crypto-currency with the SDk-optimal policy rule 3.14.

Furthermore, a higher return can be expected from the stochastically-dominant crypto-currency by the iterated deletion of strictly dominated strategies when extending Theorem 10 to the market portfolio setting. □

Finally, the efficient and strategy-proof portfolio of Theorem 20 induces an investment-efficient Nash equilibrium:

Definition 21. A mechanism M induces efficient investment within ϵ by investor $i \in I$ if, for all valuation functions $\mathbb{v}^{I\setminus\{i\}} \in \mathbb{V}^{I\setminus\{i\}}$, if

$$\hat{\mathbb{v}}^i \in \arg\max_{\tilde{\mathbb{v}}^i \in \mathbb{V}^i} \left\{ E_{\left(\mathbb{v}^i, \mathbb{v}^{I\setminus\{i\}}\right)} \left[u^i \left(M\left(v^i, v^{I\setminus\{i\}}\right); v^i \right) \right] - c^i\left(\tilde{\mathbb{v}}^i\right) \right\}$$

then we have

$$\begin{aligned} &\left(E_{\left(\hat{\mathbb{v}}^i, \mathbb{v}^{I\setminus\{i\}}\right)} \left[V\left(M\left(v^i, v^{I\setminus\{i\}}\right); \left(v^i, v^{I\setminus\{i\}}\right)\right)\right]\right) - c^i\left(\hat{\mathbb{v}}^i\right) + \epsilon \\ \geq &\sup_{\mathbb{v}^i \in \mathbb{V}^i} \left\{ \left(E_{\left(\tilde{\mathbb{v}}^i, \mathbb{v}^{I\setminus\{i\}}\right)} \left[V\left(M\left(v^i, v^{I\setminus\{i\}}\right); \left(v^i, v^{I\setminus\{i\}}\right)\right)\right]\right) - c^i\left(\tilde{\mathbb{v}}^i\right) \right\} \end{aligned}$$

for all cost functions c^i. In other words, a mechanism induces efficient investment by i within ϵ if, assuming agents report truthfully, every expected utility-maximising investment choice by i maximises expected social welfare within ϵ.

Theorem 22. *For any stochastic uncertainties $\epsilon \geq 0$ and $\eta \geq 0$, if the portfolio is approximately strategy-proof 19 within ϵ for investor i and approximately efficient within η (i.e., first-order 12, second-order 14 or SDk-efficient 16), then it induces an approximately efficient investment within $(\epsilon + \eta) \cdot (\#Crypto\text{-}currencies)$ to i, independent of the other investors' investments. Furthermore, the stochastically dominant crypto-currency induces a Nash equilibrium over the crypto-currency market that maximises ex-ante social welfare.*

Proof. Follows trivially from Theorem 5 and Corollary 2 of [HKK19]. It also holds in expectations for any given investment choice profile of the other agents using Theorem 7 from [HKK19]. □

Remark 23. **On the immovable commitment of crypto-currency monetary policy rules and the lack of discretion**: most crypto-currencies follow the example of Bitcoin, where the monetary policy was fixed since its launch and it was pre-announced that it will never change. This is in stark contrast with the monetary policy of fiat currencies, where discretion is preferred in case of a financial crisis. In other words, the widely accepted monetary policy stance of crypto-currencies to fix their monetary policies not only leaves them vulnerable to a financial crisis, but also turns them into dominated crypto-currencies by stochastically dominant crypto-currencies.

3.3.3 Omega ratio of Stochastically Dominant Crypto-currencies

The Omega ratio[KS02] is a risk-return performance measure of an asset, portfolio, or strategy which takes into account all the higher moment information in the returns distribution and also incorporates sensitivity to return levels, unlike the Sharpe ratio. It is defined as the probability-weighted ratio of gains versus losses for some threshold return target θ,

$$\Omega(\theta) = \frac{\int_{\theta}^{\infty} [1 - F(r)]\, dr}{\int_{-\infty}^{\theta} F(r)\, dr} = \frac{w^T E(r) - \theta}{E\left[(\theta - w^T r)_+\right]} + 1$$

Note that first-order stochastic dominance 11 implies Omega ratio dominance:

Theorem 24. *(Theorem 2, [GJW17]). For any two returns X and Y with means μ_X and μ_Y and Omega ratios $\Omega_X(\eta)$ and $\Omega_Y(\eta)$, respectively, if $X \leq_{SD1} Y$, then $\Omega_X(\eta) \geq \Omega_Y(\eta)$ for any $\eta \in R$.*

Corollary 25. *The efficient portfolio long on the stochastically dominant crypto-currency of Theorem 20 has a higher Omega ratio for any return threshold.*

3.3.4 Arbitraging with Stochastic Dominance

If there exists a First-order Stochastic Dominance between two assets 8, under certain conditions, arbitrage opportunities will also exist: thus investors will increase not only their expected utilities, but also their wealth if they shift their holdings to the dominant asset from the dominated one (i.e., a risk-free investment opportunity with positive returns).

Theorem 26. *(Arbitrage versus Stochastic Dominance - [Jar86]). Given a complete market M, there exists an arbitrage opportunity if and only if there exists assets x and $y \in M$ such that:*

- $x \leq_{SD1} y$
- $[P_i(y \leq \alpha) - P_i(x \leq \alpha)] \leq 0$ for all $\alpha \in \mathbb{R}$ and for some investor $i \in I$, where $P_i()$is the ith investor's subjective probability belief over the finite number of states of nature

In other words, arbitrage implies First-order Stochastic Dominance but the inverse is not necessarily true: it's only true when the cumulative distribution functions of the assets are perfectly correlated or the risky asset is a monotone function of the asset even in the absence of perfect correlation. Note that crypto-currency markets are unusually highly correlated compared to other asset markets.

In practice, empirical studies may statistically detect First-order Stochastic Dominance, but arbitrage opportunities may not exist: nonetheless, investors can increase their expected utilities, as well as their expected wealth, if they shift their holdings to the dominant asset from the dominated one [WPL08].

4 Model and Policies

DSGE models constitute the modern workhorse of monetary policy analysis, with a recent survey finding 84 models used by 58 institutions [Yag20]. In this section, a Dynamic Stochastic General Equilibrium (DSGE) parsimonious model is introduced to an economy featuring a Central-Bank Digital Currency (CBDC) and a crypto-currency, calibrated and estimated for the United States.

The model is further simplified by opting for a closed-economy instead of a small open-economy, justified by previous results showing that optimal policies under parameter uncertainty lack exchange rate responses [JP10] and that welfare loss functions for small open economies do not include foreign variables when the calibration is imposed [GM05].

4.1 Monetary Policy Rules

The following monetary policy rules are implemented in this model.

4.1.1 Central Bank

Taylor's rule for the monetary policy:

$$\begin{aligned} i_t = (\rho_2 - \rho_1)\,(\bar{i}) + \rho_1\, i_{t-1} + \rho_3\,\left(1 - \tfrac{M_{t-1}}{Y_{t-1}}\right) \\ + (\rho_2 - \rho_1)\,(\phi_\pi\,(\pi_t - \bar{\pi}) + \phi_y\,(log\,(Y_t) - log\,(Y_{t-1}))) + \epsilon_{it} \end{aligned} \tag{4.1}$$

where ρ_i are smoothing parameters and ϕ_π is the inflation feedback coefficient.

4.1.2 Bitcoin's Monetary Policy

Although Bitcoin's monetary policy is not described in its paper, its implementation appears in the source code [Nak09a]: the initial reward of 50 BTC is halved every 210,000 blocks (4 years), and each block is mined approximately every 10 minutes. The supply formula in block time is given by,

$$B(t) = \sum_{t=1}^{min(t,T)} \frac{50}{2^{H(t)}} \tag{4.2}$$

$$H(t) = \left\lfloor \frac{t}{210000} \right\rfloor \tag{4.3}$$

where t is the block height, $H(t)$ is the number of reward halvings up to block t, and $T = 33x210000$. Bitcoin supply is limited beyond block T, given by

$$B_{total} = \sum_{i=0}^{32} \frac{50}{2^i} \times 210000 \approx 2.1 \times 10^7 \tag{4.4}$$

Equation 4.2 can be fitted as an exponential curve, given by:

$$S_t^{BTC} = 2.1 \times 10^7 \times \left(1 - \alpha^t\right) \tag{4.5}$$

where S_t is the supply in period t, and α is the growth rate with $\alpha \approx 0.825$ for yearly periods and $\alpha \approx 0.953$ for quarterly periods. The previous exponential curve can be rewritten in recursive form as:

$$f_0 = 2.1 \times 10^7 \tag{4.6}$$

$$f_t = 0.825 \times f_{t-1} \tag{4.7}$$

$$S_t^{BTC} = 2.1 \times 10^7 - f_t \tag{4.8}$$

or equivalently:

$$S_{t+1}^{BTC} = S_t^{BTC} + (1 - \alpha)\left(2.1 \times 10^7 - S_t^{BTC}\right) \tag{4.9}$$

$$= \alpha \cdot S_t^{BTC} + (1 - \alpha) \cdot 2.1 \times 10^7 \tag{4.10}$$

The following figure displays the evolution of bitcoin supply assuming exact 10-minute confirmation times.

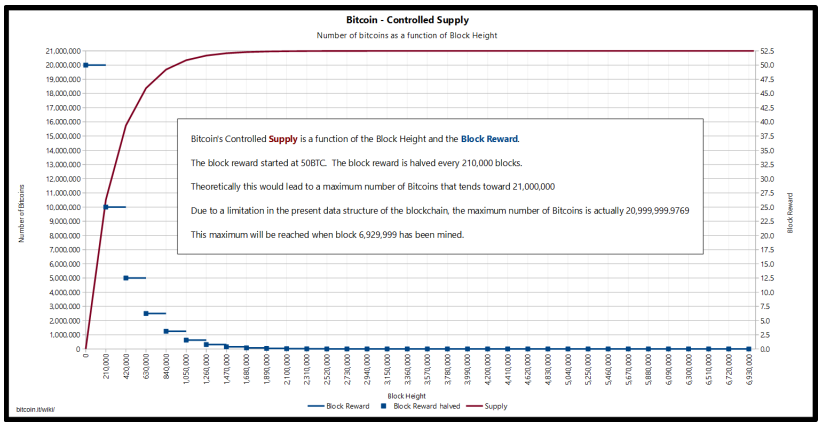

Figure 4.1: Bitcoin's controlled supply[Wik22]

As previously pointed out in Figure 2.1 comparing the relative supply of crypto-currencies, most crypto-currencies follow similar supply curves but use different parameters: therefore, without loss of generality we will only consider Bitcoin in this paper in representation of all the other crypto-currencies.

Note that Bitcoin's monetary policy is independent of any observable variable (e.g., inflation, output, ...) and Satoshi Nakamoto pre-committed not to ever modify it: in macro-economics, this monetary policy can be interpreted as a deflationary version of Friedman's k-percent rule[FS63] (i.e., constant money growth). Following Poole's classical Keynesian analysis [Poo70] in a stochastic IS-LM model, monetary policies targeting only the money stock allow money demand shocks to contribute to macroeconomic volatility: indeed, recent analysis in modern New Keynesian models [Ire00, CD05, Gal15] demonstrate that constant money growth rules lead to excess volatility in both output and inflation when the economy faces money demand shocks, or other disturbances that require output and inflation to adjust. This situation is further aggravated by an inelastic supply curve in both the short and the long term: as the following comparative chart shows 4.2, supply inelasticities imply dramatic price changes with even minor changes in demand, thus contributing to Bitcoin's volatility.

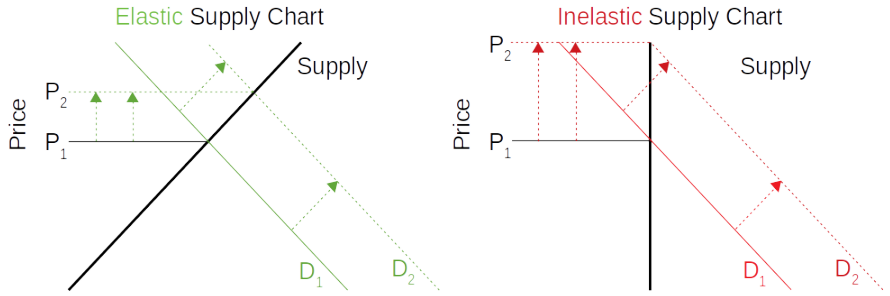

Figure 4.2: Elastic v. Inelastic Supply Charts

However, money growth rules perform much better when they are able to adjust to movements in the output gap and inflation as exemplified by the two following rules 4.11 and 4.12: advantageously, these money growth rules are able to stabilise inflation by pre-committing to an average rate of money growth and focusing directly on stabilising the output gap over shorter time horizons, instead of the aggressive responses to inflation needed by interest rate rules (i.e., Taylor's rule).

4.1.3 Ethereum 2.0's Monetary Policy

Other crypto-currencies feature a much more complex monetary policy than Bitcoin's monetary policy 4.1.2, although in essence they all suffer from the same shortcoming: they fail to react to changes in inflation, output gap, or any other macro-economic aggregate (unlike the monetary policy presented in this paper).

For the particular case of Ethereum 2.0 after transitioning to Proof-of-Stake (a.k.a., "the Merge"), the monetary policy will be described by the following features:

- almost deflationary by default: issuance reduced from 2 Ether/block to a variable number depending on the total amount of Ether at stake (currently around 13.3MM ETH), which will be around 600K ETH/year, implying a 90% reduction
- deflationary burning of transaction fees (EIP-1559)
- double use as store of value and gas for smart contracts

Accounting in a monetary policy rule for all the previous features will only make it more deflationary, thus less reactive to changes in the macro-economic environment (i.e., a narrower path of policy responses) and therefore much more stochastically dominated even than Bitcoin's monetary policy 4.1.2.

4.1.4 McCallum's Policy Rule

A classical monetarist policy, McCallum's rule [MN99] is specified by:

$$\Delta b_t = \Delta x^* - \frac{(x_{t-1} - b_{t-1} - x_{t-17} + b_{t-17})}{16} + \lambda \left(x^*_{t-1} - x_{t-1}\right) \tag{4.11}$$

where the previous variables are defined as:

- b_t is the logarithm of the adjusted monetary base
- x_t is the logarithm of the adjusted nominal GDP
- x^*_t is the target value of x_t for quarter t (growing smoothly at the rate Δx^*).

The second term provides a velocity growth adjustment intended to reflect long-lasting institutional changes, while the third term features feedback adjustment in Δb_t in response to cyclical departures of x_t from the target path x^*_t, with $\lambda \geq 0$ chosen to balance the speed of eliminating $x^*_t - x_t$ gaps against the danger of instrument instability.

4.1.5 A Reconsideration of Money Growth Rules

If the Federal Reserve would have used a money rule targeting money growth instead of the interest rate during the 2007-2009 recession, the US economy would have recovered more quickly, and during the 2009-2015 period of zero nominal interest rates, it would have stabilised output and inflation with comparable performance [BI22]. While the recent consensus was that policy rules using *constant* rates of money growth would have performed poorly in comparison to Taylor rules, recent work [BI22] shows that money growth rules augmented to adjust to movements in the output gap and inflation in a manner similar to the Taylor rule will perform significantly better, on par with more conventional Taylor rules for the interest rate. Thus, the reconsidered money growth rule is given by

$$\ln\left(\mu_t/\mu\right) = \rho_{mm} \ln\left(\mu_{t-1}/\mu\right) + \rho_{m\pi} \ln\left(\pi_t/\pi\right) + \rho_{mx} \ln\left(x_t/x\right) \tag{4.12}$$

where the previous variables are defined as:

- $\mu_t = M_t/M_{t-1}$ denotes the growth rate of nominal money
- μ denotes the steady-state rate of money growth
- π denotes the steady-state rate of inflation

- x denotes the steady-state values of the output gap

Depending on the values of the parameters, the following cases can be considered:

- $\rho_m = \rho_{m\pi} = \rho_{mx} = 0$ is the *constant* money growth rule as advocated by Friedman [FS63]
- $\rho_{m\pi} < 0$ and $\rho_{mx} < 0$ allow to stabilise inflation and the output gap in response to shocks
- $\rho_{m\pi} < 0$, $\rho_{mx} < 0$ and $\rho_{mm} > 0$ prescribe a gradual response of money growth to movements in inflation and the output gap, much like the Taylor rule with interest rate smoothing

4.2 Ranking of Policy Rules

5 Implementation Details

The calculation of the stochastically-dominant optimal monetary policy is implemented using Dynare [ABJ+22] with an additional 225.000 MATLAB/Octave LOCs.

5.1 Global Implementation

Different countries feature different macro-economic indicators (inflation, interest rate, output, GDP growth, exchange rates...), thus it is very important for the consensus protocol to be aware of the different nationalities of its participants (nodes and/or users): Pravuil [Cer21] is specifically designed for an international setting as it integrates national identity cards and biometric passports in layer 1, making it ideal to implement different monetary policies in different countries.

Furthermore, the combination of Zero-Knowledge Proof of Identity[Cer19b] with the Zero-Knowledge Stochastically Dominant crypto-currency induces the following pincer manoeuvre:

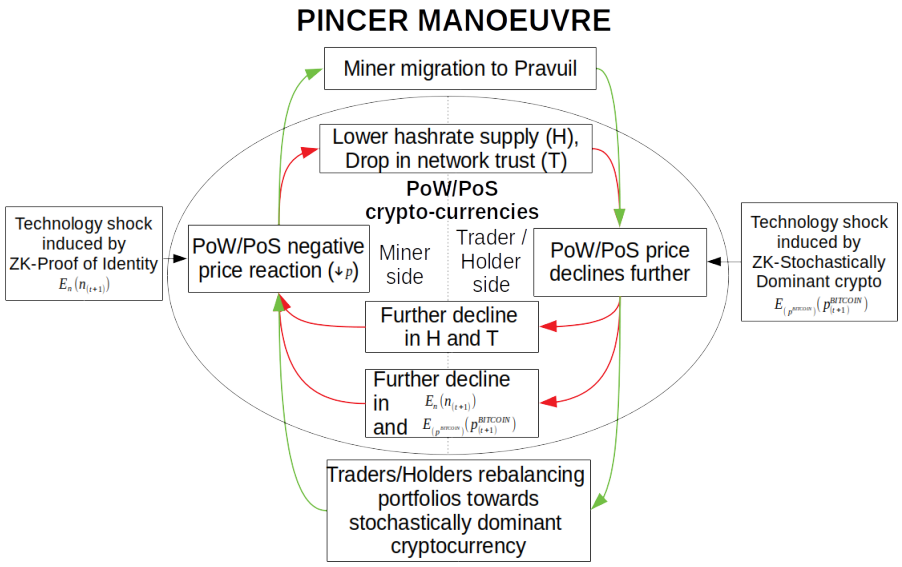

Figure 5.1: Pincer manoeuvre inducing a downward spiral on PoW/PoS crypto-currencies (in red) and a virtuous cycle for the Zero-Knowledge Stochastically Dominant crypto-currency (in green)

5.2 Zero-Knowledge Monetary Policy

To understand the reason behind the lack of advanced monetary policies in crypto-currencies as the ones described in this paper in subsections 4.1, one has to look back to a reply by Satoshi Nakamoto [Nak09b] on its original post announcing the first implementation of Bitcoin:

> *Indeed there is nobody to act as central bank or federal reserve to adjust the money supply as the population of users grows. That would have required a trusted party to determine the value, because I don't know a way for software to know the real world value of things. If there was some clever way, or if we wanted to trust someone to actively manage the money supply to peg it to something, the rules could have been programmed for that.*

Fortunately, the author of this paper is more knowledgeable: this subsection describes a zero-knowledge protocol to securely compute monetary policies using authenticated economic series and commit their resulting zero-knowledge proofs on the blockchain.

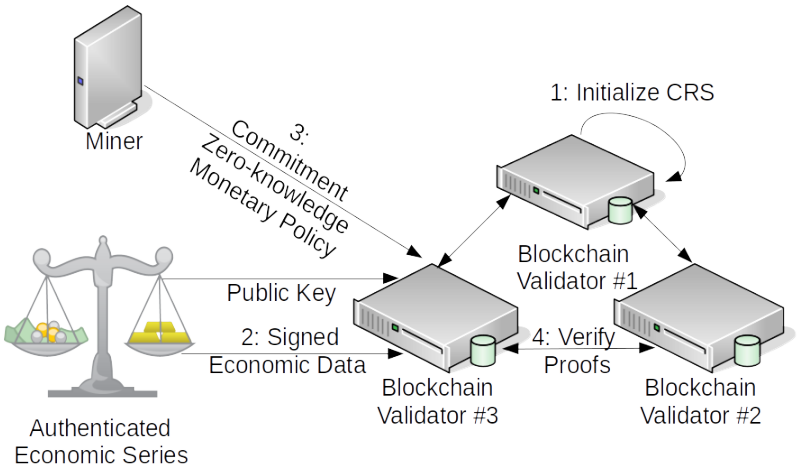

Figure 5.2: Committing zero-knowledge monetary policies on a blockchain

As pictured in the Figure 5.2 above, there are 3 parties to the protocol:

- **Miner**: commits transactions to the blockchain and gets rewarded according to a monetary policy rule using data from providers of authenticated economic series, and optionally its own private data.
- **Providers of Authenticated Economic Series**: take economic series from public providers (e.g., FRED, db.nomics, ...) and authenticate their data on the blockchain by signing with their private keys sk_{econ}, so it can later be verified by everyone with the public key pk_{econ}.
- **Blockchain Validators**: blockchain nodes that verify transactions, blocks, and proofs. As previously discussed 5.1, they should be running the Pravuil [Cer21] consensus protocol.

5.2.1 Security Model

The security model is defined with an ideal functionality $\mathcal{F}_{zkMonetaryPolicy}$ that rigorously sets the security requirements of the zero-knowledge protocol:

- **Initialisation**: the blockchain is initialised with public input data p and a computation circuit C
- **AuthenticateEconomicData**: the provider of Authenticated Economic Series sends a data authentication request to obtain the digital signature s_{econ} over (data_{public}).
- **zk-CommitMonetaryPolicy**: miners request with authenticated data containing $\text{input}_{public}, input_{private}$, the hash h of inputs, and the output_{miner}.

Ideal Functionality $\mathcal{F}_{zkMonetaryPolicy}$

$\mathcal{F}_{zkMonetaryPolicy}$ interacts with the adversary $\mathcal{A}$, the miner, the providers of authenticated economic series, the ideal functionality $\mathcal{F}_{sig}$ and the ideal blockchain ledger functionality $\mathcal{L}$ with the following queries:

- **Initialisation**: upon receiving $(init, C, p)$ on initialisation:
  - store the circuit C and the public input data p
  - send $(init, C, p)$ to $\mathcal{A}$
- **AuthenticateEconomicData**: upon receiving $(authenticate, \text{data}_{public})$ from a provider of authenticated economic series:
  - send $(sign, provider, \text{data}_{public})$ to $\mathcal{F}_{sig}$ and receives signature s_{econ}
  - send $(sign, provider, \text{data}_{public})$ to $\mathcal{A}$
- **Validate**: upon receiving $\big(validate, \text{output}_{miner}, \text{input}_{public}, \text{input}_{private}, h, s_{econ}\big)$ from a miner:
  - send $(verify, provider, h, s_{econ})$ to $\mathcal{F}_{sig}$ and check that it's correct
  - check that $\big(p, \text{output}_{miner}, \text{input}_{public}, \text{input}_{private}, h\big)$ satisfies the circuit C
  - send $\big(validate, \text{output}_{miner}, \text{input}_{public}, h, s_{econ}\big)$ to $\mathcal{A}$

The ideal functionality $\mathcal{F}_{zkMonetaryPolicy}$ captures the following design goals:

- **Authenticity**: blockchain validators execute only on resulted computations from providers of authenticated economic series, rejecting otherwise.
- **Privacy**: the private data of the miner is never exposed to anyone, and the blockchain validators are executed correctly without the private data using the zero-knowledge proof.

5.2.2 Protocol Description and Implementation

Using a zero-knowledge SNARK scheme Λ, the steps of the proposed scheme would be as follows:

- **Initialisation**: A security parameter 1^λ is picked in accordance with the security requirements, and a circuit C is constructed for the computation over the authenticated data. Then, a trusted generator or a MPC protocol setups the zk-SNARK with $\big(1^\lambda, C\big)$ to create the Common Reference String for proof generation and verification.
  Concurrently, the provider of authenticated economic series chooses a public/private key pair (pk_{econ}, sk_{econ}). Only then, (CRS, pk_{econ}) are published on the blockchain for everyone to check their validity.

- **AuthenticateEconomicData**: providers of authenticated economic series obtain signatures s_{econ} with parameters $(sk_{econ}, (h, \text{data}_{public}))$.

- **zk-CommitMonetaryPolicy**: miner uses circuit C of the monetary policy to obtain the result output_{miner} and a hash h of $\big(\text{input}_{public}, \text{input}_{private}\big)$; then, the miner executes the zk-SNARK for proving with parameters $\big(CRS, p, \text{input}_{public}, \text{input}_{private}, \text{output}_{miner}, h\big)$ obtaining the zero-knowledge proof π. Then, the miner sends a transaction to the blockchain validators as follows:

$$\text{tx}_{sk_{miner}} = \big(validate, \pi, \text{input}_{public}, \text{output}_{miner}, h\big)$$

- **Validation**: blockchain validators verify the zk-SNARK with parameters $\big(CRS, pk_{econ}, \pi, p, \text{input}_{public}, \text{output}_{miner}, h\big)$: only in case it's found valid, then the block from the miner is accepted with the computed monetary policy.

$zk - MonetaryPolicy$ **Protocol**

Miner:

- **zk-CommitMonetaryPolicy**: on input $\left(commit, p, \text{input}_{public}, \text{input}_{private}, \text{output}_{miner}, h\right)$
  - prove with zk-SNARK:

$$\pi = Prove\left(CRS, p, \text{input}_{public}, \text{input}_{private}, \text{output}_{miner}, h\right)$$

  - send $\text{tx}_{sk_{miner}} = \left(validate, \pi, \text{input}_{public}, \text{output}_{miner}, h\right)$ to the blockchain validator

Providers of Authenticated Economic Series:

- **Initialisation**:
  - $(pk_{econ}, sk_{econ}) = KeyGeneration\left(1^{\lambda}\right)$
- **Commit Authenticated Economic Data**:
  - compute $h = Hash(data_{public})$ and $s_{econ} = Sign\left(sk_{econ}, (h, data_{public})\right)$
  - send (h, s_{econ}) to the blockchain

Blockchain Validators:

- **Initialisation**: upon receiving $(init, C, p, CRS, pk_{econ})$
  - Store the public input data p for C
  - Store the common reference string CRS and pk_{econ}
- **Validation**: upon receiving $\left(validate, \pi, \text{input}_{public}, \text{output}_{miner}, h\right)$
  - Check that h is stored on the blockchain
  - Check that zk-SNARK $\left(CRS, pk_{econ}, \pi, p, \text{input}_{public}, \text{output}_{miner}, h\right)$ is valid
  - If valid, proceed to store the transactions, block, and associated zk-proof π

The following theorem formalises the security and privacy of the above scheme:

Theorem 27. *If Λ is a simulation-extractable zk-SNARK with data authentication scheme, then the above scheme is a privacy-preserving scheme under the universally composable framework.*

Proof. See I. □

Corollary 28. *In the implementation, a simulation-extractable zk-SNARK such*

as Plonk must be used [GKK+21], even if it has larger proofs than other more succinct zk-SNARKs.

An implementation in Go using gnark[BPH+22] is available at `https://github.com/Calctopia-OpenSource/cothority/tree/zkmonpolicy`

6 Conclusion

The present paper has tackled and successfully solved the problem of optimal monetary policies specifically tailored for crypto-currencies, stochastically dominating all the other previous crypto-currencies. Furthermore, the efficient portfolio is to hold the stochastically dominant crypto-currency implementing the optimal monetary policy, a strategy-proof arbitrage featuring a higher Omega ratio with a higher expected return, inducing a Nash equilibrium over the crypto-currency market.

References

[AAT21] Sofia Anyfantaki, Stelios Arvanitis, and Nikolas Topaloglou. Diversification benefits in the cryptocurrency market under mild explosivity, 2021. `https://www.sciencedirect.com/science/article/abs/pii/S0377221721001715`.

[ABJ+22] Stéphane Adjemian, Houtan Bastani, Michel Juillard, Fréderic Karamé, Ferhat Mihoubi, Willi Mutschler, Johannes Pfeifer, Marco Ratto, and Normann Rion Sébastien Villemot. Dynare: Reference Manual Version 5, 2022. `https://www.dynare.org/wp-repo/dynarewp072.pdf`.

[And08] Gary S. Anderson. Solving Linear Rational Expectations Models: A Horse Race, 2008. `http://dx.doi.org/10.1007/s10614-007-9108-0`.

[BGW14] Benjamin Blau, Todd Griffith, and Ryan Whitby. The Technology and Economic Determinants of Cryptocurrency Exchange Rates: The Case of Bitcoin, 2014. `https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2515233`.

[BGW21] Benjamin Blau, Todd Griffith, and Ryan Whitby. Inflation and Bitcoin: A descriptive time-series analysis, 2021. `https://www.sciencedirect.com/science/article/pii/S0165176521001257`.

[BI22] Michael T. Belongia and Peter Ireland. A Reconsideration of Money Growth Rules, 2022. `www.irelandp.com/papers/mgrules.pdf`.

[BK16] John Barrdear and Michael Kumhof. The Macroeconomics of Central Bank Issued Digital Currencies, 2016. `https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2811208`.

[BPH+22] Gautam Botrel, Thomas Piellard, Youssef El Housni, Ivo Kubjas, and Arya Tabaie. ConsenSys/gnark: v0.7.0, March 2022. https://doi.org/10.5281/zenodo.6387958.

[CD05] Fabrice Collard and Harris Dellas. Poole in the New Keynesian Model, 2005. https://core.ac.uk/download/pdf/6489568.pdf.

[Cer19a] David Cerezo Sánchez. Truthful and Faithful Monetary Policy for a Stablecoin Conducted by a Decentralised, Encrypted Artificial Intelligence, 2019. https://ia.cr/2019/1054.

[Cer19b] David Cerezo Sánchez. Zero-Knowledge Proof-of-Identity: Sybil-Resistant, Anonymous Authentication on Permissionless Blockchains and Incentive Compatible, Strictly Dominant Cryptocurrencies, 2019. https://eprint.iacr.org/2019/546.

[Cer21] David Cerezo Sánchez. Pravuil: Global Consensus for a United World, 2021. https://ia.cr/2021/669.

[CLL+17] Shaen Corbet, Charles Larkin, Brian Lucey, Andrew Meegan, and Larisa Yarovaya. Cryptocurrency Reaction to FOMC Announcements: Evidence of Heterogeneity Based on Blockchain Stack Position, 2017. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3073727.

[CMC21] Thomas Conlon, Richard McGee, and Shaen Corbet. Inflation and Cryptocurrencies Revisited: A Time-Scale Analysis, 2021. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3890938.

[Coh21] Gil Cohen. Trading Cryptocurrencies Using Second Order Stochastic Dominance, 2021. https://www.mdpi.com/2227-7390/9/22/2861/htm.

[CS20] Sangyup Choi and Junhyeok Shin. Brave New World? Bitcoin is not the New Gold: Understanding Cryptocurrency Price Dynamics, 2020. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3555599.

[CS21] Sangyup Choi and Junhyeok Shin. Bitcoin: An Inflation Hedge but Not a Safe Haven, 2021. https://www.sciencedirect.com/science/article/pii/S1544612321003810.

[FS63] Milton Friedman and Anna Schwartz. A Monetary History of the United States, 1867-1960, 1963. https://archive.org/details/monetaryhistoryo0000unse_y4p6.

[FV20] Jesús Fernández-Villaverde. Simple Rules for a Complex World with Artificial Intelligence, 2020. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3559378.

[Gal15] Jordi Galí. Monetary Policy, Inflation, and the Business Cycle, 2015. https://press.princeton.edu/books/hardcover/9780691164786/monetary-policy-inflation-and-the-business-cycle.

[Gal19] Alexander Galea. Crypto Monetary Base: Relative Coin Supply, 2019. https://github.com/agalea91/crypto-monetary-base.

[GJW17] Xu Guo, Xuejun Jiang, and Wing-Keung Wong. Stochastic Dominance and Omega Ratio: Measures to Examine Market Efficiency, Arbitrage Opportunity, and Anomaly, 2017. https://www.mdpi.com/2227-7099/5/4/38/pdf.

[GKK+21] Chaya Ganesh, Hamidreza Khoshakhlagh, Markulf Kohlweiss, Anca Nitulescu, and Michal Zajac. What Makes Fiat–Shamir zkSNARKs (Updatable SRS) Simulation Extractable? Cryptology ePrint Archive, Paper 2021/511, 2021. https://eprint.iacr.org/2021/511.

[GM05] Jordi Galí and Tommaso Monacelli. Monetary Policy and Exchange Rate Volatility in a Small Open Economy. *The Review of Economic Studies*, 72(3):707–734, 07 2005. https://doi.org/10.1111/j.1467-937X.2005.00349.x.

[HG16] Hanna Halaburda and Neil Gandal. Can We Predict the Winner in a Market with Network Effects? Competition in Cryptocurrency Market, 2016. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2506463.

[HKK19] John Hatfield, Fuhito Kojima, and Scott Kominers. Strategy-Proofness, Investment Efficiency, and Marginal Returns: An Equivalence, 2019. https://papers.ssrn.com/sol3/Papers.cfm?abstract_id=2544951.

[HNP+21] Weihao Han, David Newton, Emmanouil Platanakis, Charles Sutcliffe, and Xiaoxia Ye. On the (Almost) Stochastic Dominance of Cryptocurrency Factor Portfolios & Implications for Cryptocurrency Asset Pricing, 2021. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3857315.

[Hsi21] Shisong Hsiao. Monetary policy shocks and Bitcoin prices, 2021. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3947979.

[Ire00] Peter Ireland. Interest Rates, Inflation, and Federal Reserve Policy Since 1980, 2000. http://fmwww.bc.edu/EC-P/wp419.pdf.

[Jar86] Robert Jarrow. The Relationship between Arbitrage and First Order Stochastic Dominance, 1986. https://www.jstor.org/stable/2328236.

[JP10] Alejandro Justiniano and Bruce Preston. Monetary policy and uncertainty in an empirical small open-economy model. *Journal of Applied Econometrics*, 25(1):93–128, 2010. https://doi.org/10.1002/jae.1153.

[Kar21] Sören Karau. Monetary policy and Bitcoin, 2021. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3988527.

[KS02] Con Keating and William F. Shadwick. A Universal Performance Measure, 2002. http://www.performance-measurement.org/KeatingShadwick2002a.pdf.

[Lev73] Haim Levy. Stochastic Dominance, Efficiency Criteria, and Efficient Portfolios: The Multi-Period Case, 1973. https://doi.org/10.1142/9789814417358_0018.

[Lev16] Haim Levy. Stochastic Dominance: Investment Decision Making under Uncertainty, 2016. https://link.springer.com/book/10.1007/978-3-319-21708-6.

[LZ09] Li-gang Liu and Wenlang Zhang. A New Keynesian model for analysing monetary policy in Mainland China, 2009. https://www.hkma.gov.hk/media/eng/publication-and-research/research/working-papers/HKMAWP07_18_full.pdf.

[MBN20] Mourad Mroua, Slah Bahloul, and Nader Naifar. Should investors include bitcoin in their portfolio? New evidence from a bootstrap-based stochastic dominance approach, 2020. https://doi.org/10.1080/13504851.2020.1855302.

[MIOT19] Makiko Mita, Kensuke Ito, Shohei Ohsawa, and Hideyuki Tanaka. What is Stablecoin?: A Survey on Its Mechanism and Potential as Decentralized Payment Systems, 2019. https://arxiv.org/abs/1906.06037.

[MJYW14] Michel M.Denuit, Rachel J.Huang, Larry Y.Tzeng, and Christine W.Wang. Almost marginal conditional stochastic dominance, 2014. https://www.sciencedirect.com/science/article/abs/pii/S037842661300486X.

[MN99] Bennett T. McCallum and Edward Nelson. Performance of Operational Policy Rules in an Estimated Semiclassical Structural Model, 1999. http://www.nber.org/chapters/c7413.

[Nak09a] Satoshi Nakamoto. Bitcoin's initial function GetBlockValue(), 2009. https://github.com/bitcoin/bitcoin/blob/8dca7864f793072701f810e4c5ea12a6e1087085/main.cpp#L675.

[Nak09b] Satoshi Nakamoto. Re: Bitcoin open source implementation of P2P currency, 2009. http://p2pfoundation.ning.com/xn/detail/2003008:Comment:9562.

[PF21] Marco Patacca and Sergio Focardi. The Quantitative Easing Bursts Bitcoin Price, 2021. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3920808.

[PL19] Sujin Pyo and Jaewook Lee. Do FOMC and macroeconomic announcements affect Bitcoin prices?, 2019. https://doi.org/10.1016/j.frl.2019.101386.

[Poo70] William Poole. Optimal Choice of Monetary Policy Instruments in a Simple Stochastic Macro Model, 1970. https://www.bu.edu/econ/files/2011/01/PooleQJE.pdf.

[Rah20] Monireh Rahiminejat. Does Bitcoin improve optimal portfolios? A stochastic spanning approach, 2020. http://repository.bilkent.edu.tr/bitstream/handle/11693/54198/10362152.pdf.

[SY84] Haim Shalit and Shlomo Yitzhaki. Marginal Conditional Stochastic Dominance, 1984. https://www.jstor.org/stable/2632865.

[Tay20] John B. Taylor. Simple Monetary Rules: Many Strengths and Few Weaknesses, 2020. https://web.stanford.edu/~johntayl/2020_pdfs/Taylor%20paper%20for%20NYU%20conference%20Feb%2028-Paper-MCS-JBT-v2.pdf.

[TT18] Nikolas Topaloglou and Georgios Tsomidis. Investors' Behavior in Cryptocurrency Market, 2018. https://www2.aueb.gr/conferences/Crete2019/Papers/Tsomidis.pdf.

[Wik22] Bitcoin Wiki. Bitcoin's Controlled Supply, 2022. https://en.bitcoin.it/wiki/Controlled_supply.

[WPL08] Wing-Keung Wong, Kok Fai Phoon, and Hooi Hooi Lean. Stochastic dominance analysis of Asian hedge funds, 2008. https://scholars.hkbu.edu.hk/en/publications/1f0e212c-49ea-4f6d-983a-d05b22c90015.

[Yag20] Takeshi Yagihashi. DSGE Models Used by Policymakers: A Survey, 2020. https://www.mof.go.jp/pri/research/discussion_paper/ron333.pdf.

Part I
Appendix

Proof. **(Theorem 27)**. The protocol 5.2.2 securely realises the ideal functionality $\mathcal{F}_{zkMonetaryPolicy}$ 5.2.1: by using the universal composability framework, we first show an ideal-world simulator for the dummy adversary $\mathcal{A}$ automatically passing messages to and from the actual adversary, the environment $\mathcal{E}$; then, we show the indistinguishability of the ideal and the $\mathcal{F}_{sig}$-Hybrid worlds.

Ideal-world simulator. For conciseness, we only focus on the simulator $\mathcal{S}$ and not on the blockchain functionality.

- **Initialisation**: simulator $\mathcal{S}$ obtains $\widehat{CRS}$ and a trapdoor τ by running a simulated setup algorithm of the zk-SNARK scheme Λ. Then, simulator $\mathcal{S}$ keeps τ and sends $\widehat{CRS}$ to $\mathcal{E}$.

- **Simulating honest parties** (note that only **zk-CommitMonetaryPolicy** needs to be simulated): $\mathcal{E}$ sends $\big(validate, \text{output}_{miner}, \text{input}_{public}, \text{input}_{private}, h\big)$ to an honest miner and simulator $\mathcal{S}$ receives $\big(validate, \text{output}_{miner}, \text{input}_{public}, h\big)$ from the ideal functionality $\mathcal{F}_{zkMonetaryPolicy}$; then, simulator S generates an indistinguishable proof π using trapdoor τ (i.e., without knowing $\text{input}_{private}$). Finally, $\mathcal{S}$ sends $\big(validate, \pi, \text{input}_{public}, \text{output}_{miner}, h\big)$ to the blockchain validators.

- **Simulating corrupted parties**: $\mathcal{E}$ requests to the simulator $\mathcal{S}$ on behalf of corrupted parties; then $\mathcal{S}$ processes as follows: $\mathcal{S}$ receives ($validate$, output_{miner}, input_{public}, $\text{input}_{private}$, h) and extracts $\text{input}_{private}$ from the proof π using the trapdoor τ, then sends $\big(validate, \pi, \text{input}_{public}, \text{output}_{miner}, h\big)$ to $\mathcal{F}_{zkMonetaryPolicy}$.

Indistinguishability between the ideal and the $\mathcal{F}_{sig}$-Hybrid worlds: a series of games from the $\mathcal{F}_{sig}$-Hybrid protocol execution until the ideal world.

- **$\mathcal{F}_{sig}$-Hybrid model**: a dummy adversary passes messages for the environment $\mathcal{E}$, the actual adversary.

- **Hybrid** $\mathcal{H}_1$: adds to the $\mathcal{F}_{sig}$-Hybrid world calls to the simulated setup that generates τ (kept by the simulator) and $\widehat{CRS}$, sent to $\mathcal{E}$. $\mathcal{H}_1$ replaces the real proofs with the simulated proofs using $\widehat{CRS}$ and τ: due to the computational zero-knowledge property, $\mathcal{H}_1$ is computationally indistinguishable from the $\mathcal{F}_{sig}$-Hybrid world.

- **Hybrid** $\mathcal{H}_2$: adds the simulation of the blockchain to the $\mathcal{H}_1$ world. From the adversary $\mathcal{E}$'s point of view, $\mathcal{H}_2$ is indistinguishable from $\mathcal{H}_1$ because the blockchain functionality is public.

- **Hybrid** $\mathcal{H}_3$: adds to the $\mathcal{H}_2$ world, the extraction of the private witness from a zero-knowledge proof π by $\mathcal{S}$ if it is a valid proof, otherwise aborts. $\mathcal{H}_3$ is indistinguishable from $\mathcal{H}_2$ because the abort probability is negligible due to the simulation extractability property of the zk-SNARK.

Finally, the ideal and the $\mathcal{F}_{sig}$-Hybrid world are computationally indistinguishable because $\mathcal{H}_3$ is computationally indistinguishable for $\mathcal{E}$ from the ideal

simulation. Note that any universal-composable signature scheme can implement $\mathcal{F}_{sig}$ due to the universal composition theorem. □