Pravuil: Global Consensus for a United World

David Cerezo Sánchez

david@calctopia.com

22nd May 2021

Abstract

Pravuil [1] is a robust, secure, and scalable consensus protocol for a permissionless blockchain suitable for deployment in an adversarial environment such as the Internet. Pravuil circumvents previous shortcomings of other blockchains:

- Bitcoin's limited adoption problem: as transaction demand grows, payment confirmation times grow much lower than other PoW blockchains

- higher transaction security at a lower cost

- more decentralisation than other permissionless blockchains

- impossibility of full decentralisation and the blockchain scalability trilemma: decentralisation, scalability, and security can be achieved simultaneously

- Sybil-resistance for free implementing the social optimum

- Pravuil goes beyond the economic limits of Bitcoin or other PoW/PoS blockchains, leading to a more valuable and stable crypto-currency

Keywords: consensus, permissionless, permissioned, scalability, zero-knowledge, mutual attestation, zk-PoI

1 Introduction

A third generation of blockchains has been developed featuring the latest advances in cryptography and sharding to reach maximum performance and security in Internet settings: they usually make use of advances in BFT-like consensus protocols [GK18, LLS+21] and collective signatures[RGK19] to obtain 1000s of transactions per second.

In this work, we introduce Pravuil 1, a robust, secure, and scalable consensus protocol for real-world deployments on open, permissionless environments that, unlike other proposals, remains robust to high adversarial power and adaptation while considering rational participants and providing strong consistency (i.e., no forks, forward-security, and instant transactions). Our protocol is also the

---

[1]In the Book of the Secrets of Enoch[Pla26], an archangel "swifter in wisdom than the other archangels", scribe and recordkeeper.

first to integrate real-world identity on layer 1 as required by current financial regulations, obtaining Sybil-resistance for free: a very useful property considering the electrical waste produced by Bitcoin, its Achilles' heel that this blockchain circumvents for the first time by obviating to pay the Price of Crypto-Anarchy [Cer19].

To achieve the desired goals, we introduce a new consensus protocol in which we prioritise robustness against attackers and censorship-resistance. We then incorporate zero-knowledge Proof-of-Identity [Cer19] while maintaining an open, permissionless node membership mechanism enabling high levels of decentralisation. Finally, we will show a working system of the proposed design in an open-sourced Testnet at https://github.com/Calctopia-OpenSource.

1.1 Contributions

In summary, we make the following contributions:

- we propose a consensus protocol that remains robust, secure, and scalable among rational participants in an Internet setting

- we prove liveness, safety, and censorship-resistance of our new consensus protocol

- we discuss the underlying rationale of our design and prove all the advantages that it provides over previous blockchain designs

- we provide an open-source implementation running on a Testnet

2 Related Literature

Previous blockchain designs [GK18, RGK19, BMC$^+$15, LLS$^+$21] deal with the different trade-offs of the scalability trilemma (security vs. scalability vs. decentralisation) and they don't usually concern with the economic consequences of their design (e.g., the Price of Crypto-Anarchy) or the legal consequences of the lack of real-world identity as required by recent legislation (FATF's Travel Rule).

Previous designs of ByzCoin/OmniLedger/MOTOR ([KKJG$^+$16, KKJG$^+$17, KK19]) proposed Proof-of-Work(PoW) as a Sybil-resistance mechanism: although their consensus protocol is more advanced and performant than Bitcoin, they would still pay for the Price of Crypto-Anarchy [Cer19]. And although other blockchains (e.g., [DGK$^+$20]) provide methods to anonymise real-world identities, they fail to incorporate these privacy techniques on their consensus protocol as they keep on using Proof-of-Stake as a Sybil-resistance mechanism, thus they still pay the Price of Crypto-Anarchy [Cer19], suffer from Bitcoin's limited adoption problem [HJS19] and exist within the same economic limits [Bud18].

	Bitcoin	ByzCoin/MOTOR	Pravuil
Secure	✓	✓	✓
Decentralised	✓	✓	✓
Scalability	☒	✓	✓
Real-world Identity	☒	☒	✓
Free Sybil-resistance	☒	☒	✓
Lawfulness	☒	☒	✓
Unlimited adoption	☒	☒	✓
No economic limitations	☒	☒	✓

3 Background and Model

3.1 Prior Work

Pravuil builds over ByzCoin[KKJG$^+$16], OmniLedger[KKJG$^+$17], and MOTOR [KK19]: in the next section 4, we extend these protocols to address issues that prevent their deployment in an adversarial environment such as the Internet.

3.2 Assumptions

In this work, we assume the following model and definitions:

Definition 1. (Strongly-consistent broadcast [RC06]). A protocol for strong consistent broadcast satisfies the following conditions except with negligible probability:

- **Termination**: If a correct party *strongly-consistent broadcasts* m with tag ID, then all correct parties eventually *strongly-consistent deliver* m with tag ID.

- **Agreement**: If two correct parties P_i and P_j *strongly-consistent deliver* m and m' with tag ID, respectively, then $m = m'$.

- **Integrity**: Every correct party *strongly-consistent delivers* at most one payload m with tag ID. Moreover, if the sender P_s is correct, then m was previously *strongly-consistent broadcast* by P_s with tag ID.

- **Transferability**: After a correct party has *strongly-consistent delivered* m with tag ID, it can generate a string M_{ID} such that any correct party that has not *strongly-consistent delivered* message with tag ID is able to *strongly-consistent deliver* some message immediately upon processing M_{ID}.

- **Strong unforgeability**: For any ID, it is computationally infeasible to generate a value M that is accepted as valid by the validation algorithm for completing ID unless $n - 2t$ correct parties have initialised instance ID and actively participated in the protocol.

Definition 2. (Partial synchronous model [DDS83, DLS88]). In a partially synchronous network, there is a known bound Δ and an unknown Global Stabilisation Time (GST), such that after GST, all transmissions between honest nodes arrive within time Δ.

Definition 3. (n=3f+1 [FLM86]). The proportion of malicious nodes that an adversary controls accounts for no more than $1/3$ of the whole shard. The rest of the nodes are rational, that is, maximisers of their transaction rewards.

Definition 4. (Round-adaptive adversary [PS16]). We assume a mildly-adaptive, computationally bounded adversary that chooses which nodes to corrupt at the end of every consensus round and has control over them at the end of the next round.

Definition 5. (Strong Consistency [KKJG$^+$16]). The generation of each block is deterministic and instant, with the following features:

- There is no fork in a blockchain. By running a distributed consensus algorithm, state machine replication is achieved.

- Transactions are confirmed almost instantly. Whenever a transaction is written into a block, the transaction is regarded as valid.

- Transactions are tamper-proof (*forward security*). Whenever a transaction is written to a blockchain, the transaction and block cannot be tampered with and the block will remain on the chain at all times.

Definition 6. (BLS [BLS01] and BDN [BDN18] signatures). Boneh-Lynn-Sacham and Boneh-Drijvers-Neven signatures are assumed secure.

Definition 7. (Global PKI [ICA21]). Our blockchain design assumes a global PKI, not directly for consensus purposes, but as a node-admission and Sybil-resistance mechanism[Cer19].

Definition 8. (Permissionless network [SJS$^+$21]). In a permissionless network:

- Anyone can join a node without requiring permission from any party.

- Any node can join or leave at any time.

- The number of participating nodes varies at any time and is unpredictable.

4 Detailed Design

Pravuil builds over ByzCoin[KKJG$^+$16], OmniLedger[KKJG$^+$17], and MOTOR [KK19]: ByzCoin[KKJG$^+$16] envisions a Bitcoin[Nak09] protocol that uses strongly consistent consensus, scaling with multi-cast trees and aggregate Schnorr signatures. OmniLedger[KKJG$^+$17] adds sharding over ByzCoin[KKJG$^+$16], and

MOTOR[KK19] strengthens the robustness of ByzCoin[KKJG+16] for an open, adversarial network such as the Internet.

Pravuil improves over previous works by using another source of randomness, drand[DRA21a], and by incorporating zero-knowledge Proof-of-Identity[Cer19] as a Sybil-resistance mechanism into the first layer of the consensus protocol.

4.1 Goals

To sum up, Pravuil has the following goals:

- **Robustness**: the consensus round can only be disrupted by controlling the leader node.

- **Scalability**: the protocol performs well among hundreds of nodes ($n = 600$).

- **Fairness**: the malicious leader can only be elected with a probability equal to the percentage of malicious nodes in the system (i.e., the adversary cannot always control the leader).

We detail the extensions over a previous BFT protocol such as ByzCoin/MOTOR in order to obtain an improved blockchain-consensus algorithm.

4.2 Rotating Leader

View-change protocols assume a predetermined schedule of leaders, making them susceptible to adversaries that compromise the next f leaders.

To prevent this attack, our blockchain uses drand[DRA21a]: an efficient randomness beacon daemon that utilises bilinear pairing-based cryptography, t-of-n distributed key generation, and threshold BLS[BLS01] signatures to generate publicly-verifiable, unbiasable, unpredictable, highly-available, distributed randomness at fixed time intervals. As described in its online specification[DRA21c], drand uses the BLS12-381 curve, the Feldman[Fel87] Verifiable Secret Sharing protocol and the Joint Feldman protocol[GJKR99] for DKG generation; using threshold BLS signatures as a source of randomness is proven secure[GLOW20] according to its security model[DRA21b].

Remark 9. In this work, we inherit all the previous security theorems from ByzCoin[KKJG+16], OmniLedger[KKJG+17], and MOTOR [KK19].

Theorem 10. *(Robustness / Liveness). The adversary cannot predict nor bias the leader election.*

Proof. The unpredictability property follows from the unforgeability of the BLS[BLS01] signing algorithm, and the unbiasability property follows from the deterministic nature of the BLS[BLS01] signing algorithm. The leader of view v is determined by the outcomes of drand's public service, and all the nodes can publicly-verify its election when needed. Thus, the adversary cannot predict nor bias the leader election, preventing the adversary from breaking liveness. □

Theorem 11. *(Safety / Censorship-resistance). A round-adaptive adversary cannot always control the consensus decision.*

Proof. As the leader election is unpredictable (theorem 10), the adversary can only hope that one of its randomly compromised nodes gets chosen. Given that

$$\frac{1}{3^d}$$

is the probability that the adversary controls d consecutive leaders, the adversary cannot control the leader forever since

$$\lim_{d \to \infty} \frac{1}{3^d} = 0$$

thus the adversary always controls the consensus decision. □

4.3 Zero-Knowledge Proof-of-Identity

In a previous work, we introduced zero-knowledge Proof-of-Identity[Cer19] for biometric passports [ICA21] and electronic identity cards to permissionless blockchains in order to remove the inefficiencies of Sybil-resistant mechanisms such as Proof-of-Work [Nak09] and Proof-of-Stake [KN12]. Additionally, attacks [RMD$^+$20, AAM21] on PoW sharded permissionless blockchains are prevented with zk-PoI: an identity will be the same on all the shards, and the attacker can't mine new identities for different shards as it's possible on PoW blockchains.

Although some could consider the latest zero-knowledge implementations fast enough, their implementations are still too experimental for production. For the first release, we will use the SGX implementation based on mutual attestation, which works as follows (more details on the original paper [Cer19]):
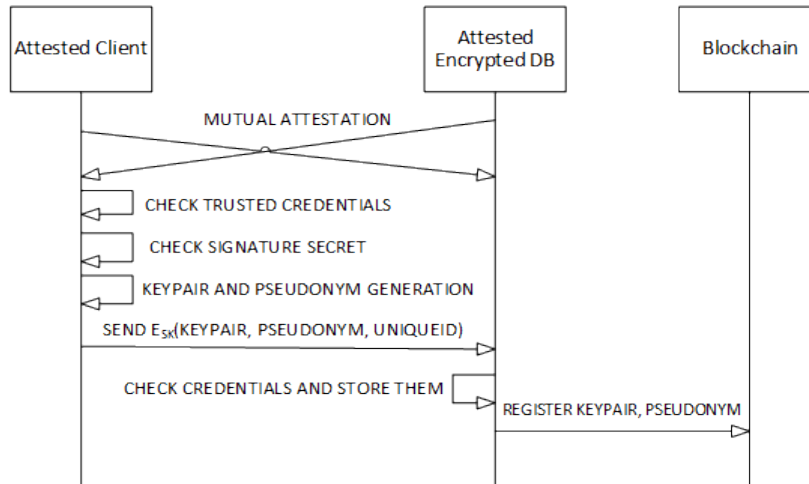

Figure 4.1: Simplified overview of mutual attestation protocol.

An approximate picture of the worldwide coverage follows:
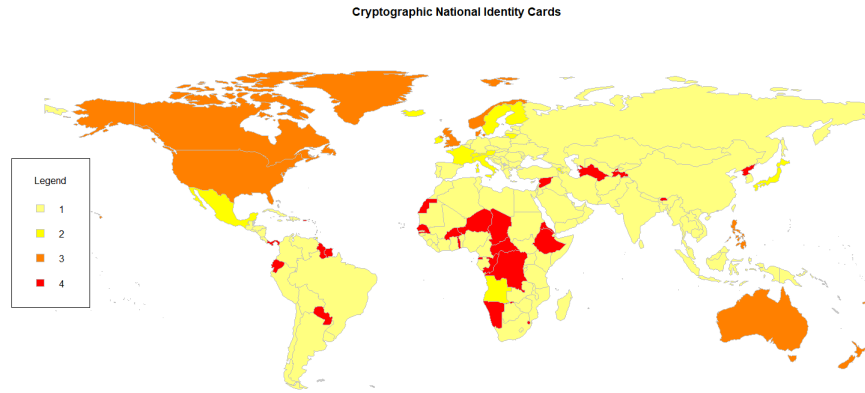
Cryptographic National Identity Cards

Figure 4.2: Legend: 1) National identity card is a mandatory smartcard; (2) National identity card is a voluntary smartcard; (3) No national identity card, but cryptographic identification is possible using an ePassport, driving license and/or health card; (4) Non-digital identity card.

5 Discussion

In this section, we discuss the economic rationale underpinning the unique features of this blockchain design that helps it to overcome previous shortcomings and achieve an improved blockchain tailored to real-world settings according to the experiences from the last decade (e.g., Bitcoin[Nak09]).

5.1 Overcoming Bitcoin's Limited Adoption Problem

In a recent paper[HJS19], it is shown that a PoW payments blockchain (i.e., Bitcoin) cannot simultaneously sustain a large volume of transactions and a non-negligible market share:

Proposition 12. *(Adoption Problem [HJS19]). Adoption decreases as demand rises (i.e., the adoption rate of a network, c^*, decreases in N). Moreover, the blockchain faces limited adoption,*

$$\lim_{N \to \infty} c^* = 0.$$

Even allowing dynamic PoW supply (i.e., by relaxing PoW's artificial supply constraint) achieves widespread adoption only at the expense of decentralisation:

Proposition 13. *(Decentralisation implies Limited Adoption [HJS19]). PoW blockchains necessarily face either centralisation,*

$$\lim_{N \to \infty} \sup V \leq 1,$$

or limited adoption,

$$\lim_{N \to \infty} c^* = 0.$$

The previous propositions expose that the lack of widespread adoption constitutes an intrinsic property of PoW payments blockchains: as transaction demands grow, fees increase endogenously. Attracted by this growth, more nodes join the validation process, expanding the network size and thus protracting the consensus process and generating increased payment confirmation times: only users insensitive to wait times would transact in equilibrium, and limited adoption arises. Moreover, this limitation cannot be overcome as it's rooted in physics (i.e., network delay).

As pointed out by the previous proposition, centralised blockchains overcome the limited adoption problem: for example, permissioned blockchains that remain secure on an open, adversarial network such as the blockchain proposed in this paper, enabling lower payment confirmation times when omitting PoW's artificial supply constraint ,

Proposition 14. *(Lower Payment Confirmation Times [HJS19]). For any PoW protocol, there exists a permissioned blockchain that remains secure on an open, adversarial network (i.e., Pravuil), which induces (weakly) lower payment confirmation times.*

Additionally, omitting PoW's artificial supply constraint facilitates timely service even for high transaction volumes:

Proposition 15. *(No Limited Adoption Problem [HJS19]). In any permissioned equilibrium, widespread adoption can be obtained,*

$$\lim_{N \to \infty} c_P^* = \min \left\{ \frac{R_P}{\Delta (V_P)}, 1 \right\}.$$

5.2 Obtaining Higher Transaction Security At A Lower Cost

In another recent paper[BH21], it is shown that permissioned blockchains have a higher level of transaction safety than a permissionless blockchain, independent of the block reward and the current exchange rate of the crypto-currency.

For a PoW permissionless blockchain, let R be the block reward in the corresponding crypto-currency, x the associated exchange rate to fiat currency, w the block maturation rate (e.g., for Bitcoin, $R = 6,25; x = \$60.000; w = 100$), f be the probability of detecting that blocks have been replaced, and β_{pl} be the value above which transactions are not safe,

$$\beta_{pl} = fwRx.$$

Note that 51% attacks are becoming more common, specially for purely financial reasons [SSVK20]. For a permissioned blockchain, let P_i be the punishment applied to each node i if it participates in an attack,$\tau \in [0, 1]$ be the probability that nodes that participated in an attack will be punished, and β_P be the value above which transactions are not safe,

$$\beta_P = f\tau \sum_{i \in B} P_i,$$

with B being the set of N nodes with the lowest P_i. Typical punishments include confiscating all the funds deposited on the blockchain and banning them from the blockchain, among others.

Proposition 16. *([BH21]). A permissioned blockchain that is safe in an open, adversarial environment (i.e., Pravuil) has a higher level of maximum value for transaction safety than a PoW permissionless blockchain if*

$$\tau \sum_{i \in B} P_i > wRx.$$

Even with small values of τ will result in higher safety for larger transactions than PoW permissionless blockchains:

Proposition 17. *([BH21]). For $\tau > 0$ and high enough P_i's, a permissioned blockchain that is safe in an open, adversarial environment (i.e., Pravuil) is more resilient than PoW permissionless blockchains whenever*

$$\sum_{i \in B} P_i > \frac{wRx}{\tau}.$$

Ultimately, the cost of providing incentives to the validating nodes not to participate in potential attacks (i.e., validating incentives such as block rewards) will be lower for permissioned blockchains.

Proposition 18. *([BH21]). Suppose that $\beta_{pl} > 0$ and $\beta_p > 0$, then at equilibrium the validator incentives in the permissioned blockchain that is safe in an open, adversarial environment (i.e., Pravuil) are lower than for the PoW permissionless.*

According to the model of this paper, in order to increase the transaction safety, we only need to need increase:

- τ, a probability that reflects user's trust in the system

- P_i, a penalty that could also include legal action

In general, the mere existence of credible penalties P_i with positive probability τ is enough for the system to remain secure, without needing to exert punishments in the case of rational attackers. Additionally, note that these parameters are not economic parameters of the system, unlike the parameters for PoW permissionless blockchains.

5.3 An Empirical Approach to Blockchain Design

Motivated by the abstract analysis from the previous sub-section 5.2, we use the numerical comparisons between crypto-currencies from the paper [GAR18] to compare permissionless and permissioned blockchains in practice:

	BTC	ETH	BCH	LTC	ADA	USDT	Mean
Popularity	1	2	4	7	8	9	
Cost	1.33	2	1.66	2.66	4.33	5	2.83(*)
Consistency	1.33	2.33	1.33	2	3.66	1	
Functionality	2	5	2	2	4.33	2	
Performance	1.33	1.66	2	2.33	3	1	1.88(*)
Security	4	4	4	4	4	3.33	3.88
Decentralisation	5	3.33	4.33	3.66	3.33	1.33	
Total	14.99	18.32	15.32	16.7	22.65	13.66	
Performance/Cost	0.28	0.41	0.46	0.7	1.79	1	0.77(*)
(Perf*Sec)/Cost	1.13	1.66	1.84	2.79	7.18	3.33	2.99(*)
Security/Cost	0.85	1	0.92	1.2	2.39	3.33	1.61(*)

Table 1: Permissionless blockchains. (*): $p < 0.05$

	XRP	EOS	XLM	TRX	MIOTA	Mean
Popularity	3	5	6	11	10	
Cost	4.66	5	4.66	5	5	4.84(*)
Consistency	4.33	5	4	4	4.66	
Functionality	1.33	5	1.33	5	3.66	
Performance	4.33	4.66	4	4.66	5	4.53(*)
Security	2.33	3.33	4	3.33	3.66	3.33
Decentralisation	1	2.66	2.33	3.33	2.33	
Total	17.98	25.65	20.32	25.32	24.31	
Performance/Cost	3.23	4.66	2.98	4.66	5	4.10(*)
(Perf*Sec)/Cost	7.52	15.51	11.94	15.51	18.3	13.76(*)
Security/Cost	1.73	3.33	2.98	3.33	3.66	3(*)

Table 2: Permissioned blockchains. (*): $p < 0.05$

Using two-samples t-tests assuming unequal variances, we compare the following means between permissionless and permissioned blockchains, remarking that they are statistically significant:

- **Cost**: permissionless blockchains are costlier (2.83) than permissioned blockchains (4.84). Please note that a higher cost score means that the blockchain is considered to have better costs (i.e., lower costs), and the

ranking obtained from this cost score must be reversed to be useful in the next rankings.

- **Performance**: permissionless blockchains are less performant (1.88) than permissioned blockchains (4.53).

- **Performance/Cost**: permissionless blockchains show worse performance regarding cost (0.77) than permissioned blockchains (4.10).

- **(Performance*Security)/Cost**: permissionless blockchains show worse performance and security regarding cost (2.99) than permissioned blockchains (13.76).

- **Security/Cost**: permissionless blockchains show worse security regarding cost (1.61) than permissioned blockchains (3).

It's clear from the empirical data that permissionless blockchains are considered worse than permissioned blockchains when considering cost, performance and security.

5.4 Achieving More Decentralisation Than Other Permissionless Blockchains

In yet another recent publication [BHMB21], it is noticed that permissioned blockchains could achieve more decentralisation than permissionless blockchains: real-world permissionless blockchains are quite centralised [GBE+18], as there aren't formal checks for the underlying centralisation.

In order to obtain a more decentralised permissioned blockchain that is safe in an open, adversarial network (i.e., Pravuil), the node admission/gatekeeping function must be decentralised and opened: precisely, this ideal state is achieved with our zero-knowledge Proof-of-Identity [Cer19], as previously explained in sub-section 4.3.
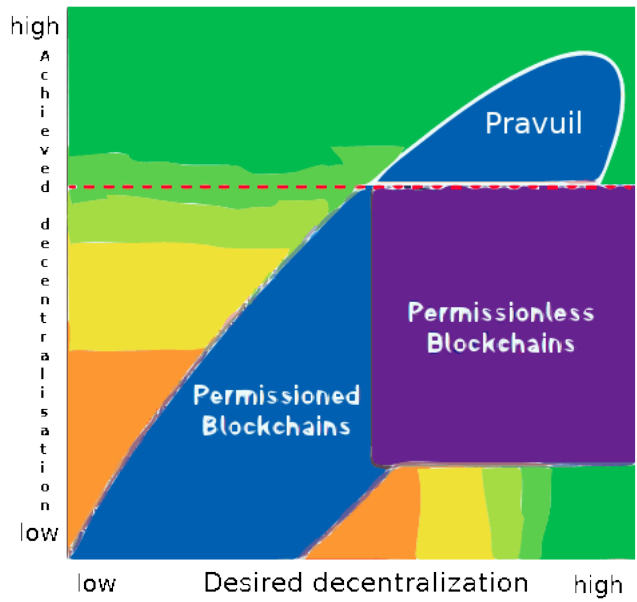
Figure 5.1: Comparing decentralisation (from [BHMB21]).

5.5 Overcoming The Scalability Trilemma

The scalability trilemma postulates that a blockchain system can only at most have two of the following three properties: decentralisation, scalability, and security.
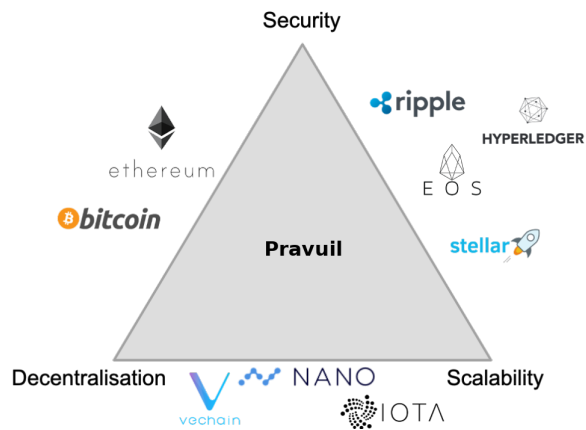

Figure 5.2: Pravuil overcomes the Scalability Trilemma.

12

In Pravuil, decentralisation, scalability, and security can be achieved simultaneously:

- **Decentralisation**: as discussed in the previous sub-section 5.4, Pravuil can be more decentralised than other permissionless blockchains by using zero-knowledge Proof-of-Identity, as previously explained in sub-section 4.3. It also circumvents the impossibility of full decentralisation [Cer19].

- **Scalability**: Pravuil inherits the scalable *Rotating-Subleader* (RS) communication pattern from MOTOR [KK19], specifically created to avoid the communication bottleneck experienced by classic BFT protocol when run over limited bandwidth networks.

- **Security**: Pravuil is secure as previously proved in theorem 10 and theorem 11.

5.6 Obviating the Price Of Crypto-Anarchy of PoW/PoS Crypto-currencies

In a previous paper [Cer19], it was pointed out that the most cost-efficient Sybil-resistant mechanism is the one provided by a trusted national PKI infrastructure [Dou02] and a centralised social planner would prefer the use of National Identity Cards and/or ePassports in order to minimise costs: instead, permissionless blockchains are paying very high costs by using PoW/PoS as Sybil-resistant mechanisms. The Price of Crypto-Anarchy compares the ratio between the worst Nash equilibrium of the congestion game defined by PoW blockchains and the optimal centralised solution, quantifying the costs of the selfish behaviour of miners.

Definition. (#26 from [Cer19]). Let $NashCongestedEquil \subseteq S$ be the set of strategies given as the solution of the optimisation problem of Theorem 25 from [Cer19], then the *Price of Crypto-Anarchy* is given by the following ratio:

$$\text{Price of Crypto-Anarchy} = \frac{\max_{s \in NashCongestedEquil} Cost\,(s)}{Cost\,(\text{zk-PoI})}$$

In practice, the real-world costs of Zero-Knowledge Proof-of-Identity are almost zero as the identity infrastructure is subsidised by governments. However, the situation for PoW/PoS blockchains is quite the opposite:

- PoW blockchains: in 2018, Bitcoin, Ethereum, Litecoin and Monero consumed an average of 17, 7, 7 and 14 MJ to generate one US\$ [KT18], and in 2021 Bitcoin may be consuming as much energy as all data centers globally [Dig21, dV21] at 100-130 TWh per year. Holders of crypto-currency ultimately experience the Price of Crypto-Anarchy as inflation from mining rewards, see next Table 3:

Name	Reward per block	Block time	Blocks per day	Price	**Yearly mining reward**	**Yearly Inflation**
BTC	6,25	10 m	144	$50000	**$18,061 B**	**4,12%**
ETH	2	13,2 s	6545	$3780	**$16,425 B**	**1,76%**
DOGE	10,000	1 m	1440	$0,49	**$2,575 B**	**4,06%**
LTC	12,5	2,5 m	576	$320	**$840 MM**	**3,94%**
BCH	6,25	10 m	144	$1275	**$418 MM**	**1,75%**
ZEC	3,125	75 s	1152	$301	**$395 MM**	**11,84%**
XMR	1,02	2 m	720	$407	**$109 MM**	**1,5%**

Table 3: Empirical Price of Crypto-Anarchy.

- PoS blockchains: in theory, the costs are identical to the cost of PoW schemes, except that instead of electrical resources and mining chips, it takes the form of illiquid financial resources[GG19] and in practice, Proof-of-Stake is not strictly better than Proof-of-Work as the distribution of the market shares between both technologies has been shown to be indistinguishable (Appendix 3, [EAK+17]).

Bitcoin miners have earned a total of $26.75B as of April 2021: it's not necessary to pay so much for Sybil resistance, instead, miners could be paid for other tasks (e.g., transaction fees). As previously discussed, obtaining Sybil-resistance for free is not only the key to overcome Bitcoin's limited adoption problem (section 5.1) and to achieve more decentralisation than other permissionless blockchains (section 5.4), but also to go beyond the economic limits of Bitcoin as discussed in the next section 5.7.

5.7 Beyond the Economic Limits of Bitcoin

In a paper about the economic limits of Bitcoin [Bud18], it is pointed out that Bitcoin is prohibitively expensive to run because the recurring, "flow", payments to miners for running the blockchain (particularly, the cost of PoW mining) must be large relative to the one-off, "stock", benefits of attacking it. Let V_{attack} be the expected payoff to the attacker, P_{block} be the block reward to the miner and α representing the duration of the attack net of block rewards, then

$$P_{block} > \frac{v_{attack}}{\alpha},$$

placing serious economic constraints to the practicality and scalability of the Bitcoin blockchain, a problem that seems intrinsic to any anonymous, decentralised blockchain protocol. Consequently, the author poses the open question of finding another approach to generating anonymous, decentralised trust in a

public ledger that is less economically expensive: indeed, the technical solution hereby presented4.3 that incorporates zero-knowledge Proof-of-Identity[Cer19] is the technology that is both "scarce and non-repurposable", affordable and not susceptible to sabotage attacks that could cause a collapse in the economic value of the blockchain that the author of [Bud18] would seem meritorious to close said open question.

A more recent paper [GG19] continues the previous economic analysis [Bud18], extending it to PoS and permissioned settings. For the permissionless PoS setting, it finds that the costs are identical to the cost of PoW schemes, except that instead of electrical resources and mining chips, it takes the form of illiquid financial resources; however, zk-PoI[Cer19] is free. For the permissioned case concerning this paper, if the block reward is set exogenously, it finds that a permissioned blockchain would have lower costs than permissionless PoW or PoS blockchains in the economic model of [Bud18].

5.8   More Valuable and Stable Crypto-currencies

A review of previous literature in economic research reveals the following interesting facts regarding the intricate relationship between PoW mining (i.e., hashrate, electricity and/or equipment costs) and crypto-currency prices:

- There is a positive relationship between mining hashrate and price [GPB+15, Hay16]: the causality is primarily unidirectional going from the price to the hashrate [FK20], although mining incidents and political shocks that affect mining also negatively impact prices.

- Bitcoin's security is sensitive (elastic) to mining rewards and costs, although temporary mining cost and price shocks do not affect the long-run blockchain security [CdKR21]: a 1% permanent increase in the mining reward increases the underlying blockchain security by 1.38% to 1.85% in the long-run; positive shocks to electricity prices in China have a negative impact on the hashrate in the short-run; a 1% increase in the efficiency of mining equipment increases the computing capacity between 0.23% and 0.83% in the long-run; in the short-run mining competition intensity has a statistically positive impact leading to expansion of mining capacity, but in the long-run, the relationship is reversed.

- High fixed mining rewards are the source of the instability to reach an equilibrium between miners and users [Iyi18]; instead, mining rewards should be adjusted dynamically.

- The production of crypto-currency by miners is jointly determined with the price used by consumers [PB18]: the equilibrium price depends on both consumer preferences (i.e., price increases with the average value of censorship aversion, and current and future size of the network) and the industrial organisation of the mining market (i.e., price increases with the number of miners and decreases with the marginal cost of mining). Price-security spirals amplify demand and supply shocks: for example, a sudden

demand shock provoked by a government banning the crypto-currency in a country would lead to price drops, itself leading to miners decreasing hashrate, further decreasing prices and the feedback loop continuing until a new equilibrium is reached in multiple rounds. In other words, Bitcoin's security model embeds price volatility amplification.

- In a PoW blockchain, it's impossible to simultaneously achieve all the three following goals [Pag20]: maximise crypto-currency price, blockchain's security, and social welfare.

Similar results can be found for PoS blockchains because they are substituting electricity and mining costs for illiquid and volatile financial resources [GG19]. In general, the interdependencies can be described graphically as the following cycles and spirals:
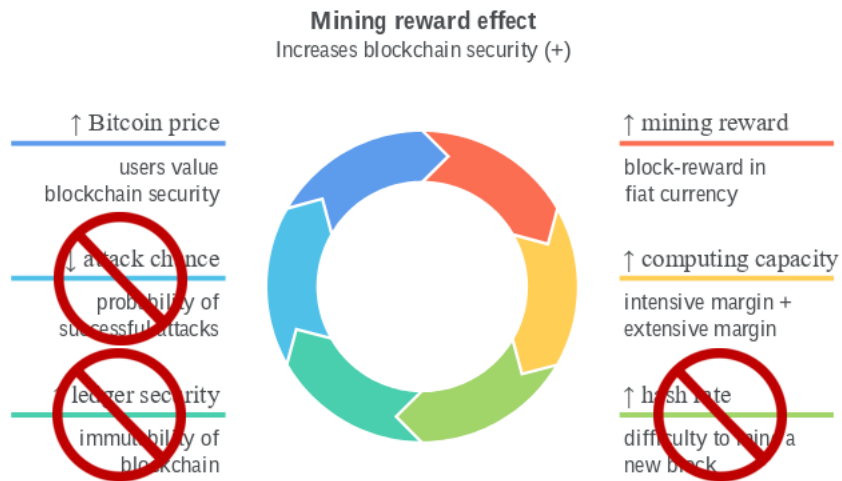

Figure 5.3: Interdependencies [CdKR21], with broken negative feedback loops.
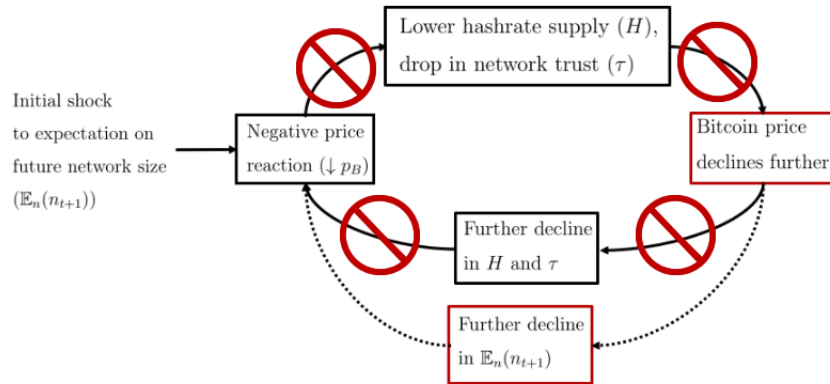
Figure 5.4: Spirals [PB18], with broken negative feedback loops.

However, we break most of the previous interdependencies and spirals with our strongly-consistent blockchain with free Sybil-resistance:

- blockchain and transaction security are independent of blockchain mining capacity, mining costs and rewards, and price: once a transaction is instantly committed, it's committed forever.

- there aren't price-security spirals for demand and supply shocks: changes in prices do not lead to changes in security.

- as blockchain's security is independent of price, it's possible to maximise crypto-currency price and social welfare.

Ultimately, our blockchain design leads to more valuable and stable crypto-currencies.

6 Implementation

Pravuil has a Testnet deployed with a working implementation consisting of:

- a blockchain layer in Go and Java, invoking drand [DRA21a] as described in this paper 4.2.

- zero-knowledge Proof-of-Identity [Cer19] in Python and C.

- mobile apps for Android (Typescript, Java) and iOS (Typescript, Objective-C, Swift).

- secure smart contracts in Obliv-Java [Cer17].

All the code will be open-sourced at https://github.com/Calctopia-OpenSource, including future developments.

7 Conclusion

In this work, we presented Pravuil, an improvement over previous blockchains that is suitable for real-world deployment in adversarial networks such as the Internet. Pravuil achieves this feat by:

- unpredictably rotating leaders using drand [DRA21a] to defend against adversaries and censorship attacks: drand is an Internet service that generates publicly-verifiable, unbiasable, unpredictable, highly-available, distributed randomness at fixed time intervals.

- using for the first time zero-knowledge Proof-of-Identity [Cer19] as a Sybil-resistance mechanism to overcome Bitcoin's limited adoption problem[HJS19] and to go beyond the economic limits of Bitcoin[Bud18], delivering more decentralisation than other permissionless blockchains [BHMB21].

- based on the design of a blockchain layer that scales-out with strong consistency prioritising robustness over scalability.

References

[AAM21]   Hafid Abdelatif, Senhaji Hafid Abdelhakim, and Samih Mustapha. A Tractable Probabilistic Approach to Analyze Sybil Attacks in Sharding-Based Blockchain Protocols, 2021. `https://arxiv.org/abs/2104.07215`.

[BDN18]   Dan Boneh, Manu Drijvers, and Gregory Neven. Compact Multi-Signatures for Smaller Blockchains. Cryptology ePrint Archive, Report 2018/483, 2018. `https://eprint.iacr.org/2018/483`.

[BH21]   Yannis Bakos and Hanna Halaburda. Tradeoffs in Permissioned vs Permissionless Blockchains: Trust and Performance, 2021. `https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3789425`.

[BHMB21]   Yannis Bakos, Hanna Halaburda, and Christoph Mueller-Bloch. When Permissioned Blockchains Deliver More Decentralization Than Permissionless, 2021. `https://cacm.acm.org/magazines/2021/2/250073-when-permissioned-blockchains-deliver-more-decentralization-than-permissionless/fulltext`.

[BLS01]   Dan Boneh, Ben Lynn, and Hovav Shacham. Short Signatures from the Weil Pairing. In Colin Boyd, editor, *Advances in Cryptology — ASIACRYPT 2001*, pages 514–532, Berlin, Heidelberg, 2001. Springer Berlin Heidelberg. `https://www.iacr.org/archive/asiacrypt2001/22480516.pdf`.

[BMC+15]   Joseph Bonneau, Andrew Miller, Jeremy Clark, Arvind Narayanan, Joshua Kroll, and Edward Felten. SoK: Research Perspectives and Challenges for Bitcoin and Cryptocurrencies,

2015. https://www.ieee-security.org/TC/SP2015/papers-archived/6949a104.pdf.

[Bud18]   Eric Budish. The Economic Limits of Bitcoin and the Blockchain, 2018. https://www.nber.org/system/files/working_papers/w24717/w24717.pdf.

[CdKR21]   Pavel Ciaian, d'Artis Kancs, and Miroslava Rajcaniova. Interdependencies between Mining Costs, Mining Rewards and Blockchain Security, 2021. https://arxiv.org/abs/2102.08107.

[Cer17]   David Cerezo Sánchez. Raziel: Private and Verifiable Smart Contracts on Blockchains. Cryptology ePrint Archive, Report 2017/878, 2017. https://eprint.iacr.org/2017/878.

[Cer19]   David Cerezo Sánchez. Zero-Knowledge Proof-of-Identity: Sybil-Resistant, Anonymous Authentication on Permissionless Blockchains and Incentive Compatible, Strictly Dominant Cryptocurrencies. Cryptology ePrint Archive, Report 2019/546, 2019. https://eprint.iacr.org/2019/546.

[DDS83]   Danny Dolev, Cynthia Dwork, and Larry Stockmeyer. On the Minimal Synchronism Needed for Distributed Consensus, 1983. https://groups.csail.mit.edu/tds/papers/Stockmeyer/DolevDS83-focs.pdf.

[DGK⁺20]   Ivan Damgård, Chaya Ganesh, Hamidreza Khoshakhlagh, Claudio Orlandi, and Luisa Siniscalchi. Balancing Privacy and Accountability in Blockchain Identity Management. Cryptology ePrint Archive, Report 2020/1511, 2020. https://eprint.iacr.org/2020/1511.

[Dig21]   Digiconomist. Bitcoin may consume as much energy as all data centers globally, 2021. https://digiconomist.net/bitcoin-may-consume-as-much-energy-as-all-data-centers-globally.

[DLS88]   Cynthia Dwork, Nancy Lynch, and Larry Stockmeyer. Consensus in the Presence of Partial Synchrony, 1988. https://groups.csail.mit.edu/tds/papers/Lynch/jacm88.pdf.

[Dou02]   John Douceur. The Sybil Attack. In *Proceedings of 1st International Workshop on Peer-to-Peer Systems (IPTPS)*, January 2002. https://www.microsoft.com/en-us/research/wp-content/uploads/2002/01/IPTPS2002.pdf.

[DRA21a]   DRAND. DRAND, 2021. https://drand.love.

[DRA21b]   DRAND. DRAND Security Model, 2021. https://drand.love/docs/security-model.

[DRA21c]   DRAND. DRAND Specification, 2021. `https://drand.love/docs/specification`.

[dV21]   Alex de Vries. Bitcoin Boom: What Rising Prices Mean for the Network's Energy Consumption, 2021. `http://dx.doi.org/10.1016/j.joule.2021.02.006`.

[EAK+17]   Abeer ElBahrawy, Laura Alessandretti, Anne Kandler, Romualdo Pastor-Satorras, and Andrea Baronchelli. Evolutionary dynamics of the cryptocurrency market, 2017. `https://arxiv.org/abs/1705.05334`.

[Fel87]   Paul Feldman. A Practical Scheme for Non-Interactive Verifiable Secret Sharing. In *Proceedings of the 28th Annual Symposium on Foundations of Computer Science*, SFCS '87, page 427–438, USA, 1987. IEEE Computer Society. `https://www.cs.umd.edu/~gasarch/TOPICS/secretsharing/feldmanVSS.pdf`.

[FK20]   Dean Fantazzini and Nikita Kolodin. Does the Hashrate Affect the Bitcoin Price?, 2020. `https://doi.org/10.3390/jrfm13110263`.

[FLM86]   Michael Fisher, Nancy Lynch, and Michael Merritt. Easy impossibility proofs for distributed consensus problems, 1986. `https://groups.csail.mit.edu/tds/papers/Lynch/FischerLynchMerritt-dc.pdf`.

[GAR18]   Martin Garriga, Maximiliano Arias, and Alan De Renzis. Blockchain and Cryptocurrency: A comparative framework of the main Architectural Drivers, 2018. `https://arxiv.org/abs/1812.08806`.

[GBE+18]   Adem Efe Gencer, Soumya Basu, Ittay Eyal, Robbert van Renesse, and Emin Gün Sirer. Decentralization in Bitcoin and Ethereum Networks, 2018. `https://arxiv.org/abs/1801.03998`.

[GG19]   Joshua S. Gans and Neil Gandal. More (or less) economic limits of the blockchain, 2019. `https://www.nber.org/system/files/working_papers/w26534/w26534.pdf`.

[GJKR99]   Rosario Gennaro, Stanislaw Jarecki, Hugo Krawczyk, and Tal Rabin. Secure Distributed Key Generation for Discrete-Log Based Cryptosystems. In *Advances in Cryptology - EUROCRYPT '99, International Conference on the Theory and Application of Cryptographic Techniques*, volume 1592 of *Lecture Notes in Computer Science*, pages 295–310. Springer, 1999. `https://link.springer.com/content/pdf/10.1007/s00145-006-0347-3.pdf`.

[GK18]   Juan Garay and Aggelos Kiayias. SoK: A Consensus Taxonomy in the Blockchain Era. Cryptology ePrint Archive, Report 2018/754, 2018. `https://eprint.iacr.org/2018/754`.

[GLOW20]   David Galindo, Jia Liu, Mihai Ordean, and Jin-Mann Wong. Fully Distributed Verifiable Random Functions and their Application to Decentralised Random Beacons. Cryptology ePrint Archive, Report 2020/096, 2020. https://eprint.iacr.org/2020/096.

[GPB+15]   Ifigeneia Georgoula, Demitrios Pournarakis, Christos Bilanakos, Dionisios Sotiropoulos, and George M. Giaglis. Using Time-Series and Sentiment Analysis to Detect the Determinants of Bitcoin Prices, 2015. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2607167.

[Hay16]   Adam S. Hayes. Cryptocurrency value formation: An empirical study leading to a cost of production model for valuing bitcoin, 2016. https://doi.org/10.1016/j.tele.2016.05.005.

[HJS19]   Franz J. Hinzen, Kose John, and Fahad Saleh. Bitcoin's Fatal Flaw: The Limited Adoption Problem, 2019. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3334262.

[ICA21]   ICAO. ICAO Public Key Directory (PKD), 2021. https://www.icao.int/Security/FAL/PKD/Pages/default.aspx.

[Iyi18]   Engin Iyidogan. An Equilibrium Model of Blockchain-Based Cryptocurrencies, 2018. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3152803.

[KK19]   Eleftherios Kokoris-Kogias. Robust and Scalable Consensus for Sharded Distributed Ledgers. Cryptology ePrint Archive, Report 2019/676, 2019. https://eprint.iacr.org/2019/676.

[KKJG+16]   Eleftherios Kokoris-Kogias, Philipp Jovanovic, Nicolas Gailly, Ismail Khoffi, Linus Gasser, and Bryan Ford. Enhancing Bitcoin Security and Performance with Strong Consistency via Collective Signing, 2016. https://arxiv.org/abs/1602.06997.

[KKJG+17]   Eleftherios Kokoris-Kogias, Philipp Jovanovic, Linus Gasser, Nicolas Gailly, Ewa Syta, and Bryan Ford. OmniLedger: A Secure, Scale-Out, Decentralized Ledger via Sharding. Cryptology ePrint Archive, Report 2017/406, 2017. https://eprint.iacr.org/2017/406.

[KN12]   Sunny King and Scott Nadal. PPCoin: Peer-to-Peer Crypto-Currency with Proof-of-Stake, 2012. https://www.peercoin.net/whitepapers/peercoin-paper.pdf.

[KT18]   Max J. Krause and Thabet Tolaymat. Quantification of energy and carbon costs for mining cryptocurrencies, 2018. https://doi.org/10.1038/s41893-018-0152-7.

[LLS+21]   Yizhong Liu, Jianwei Liu, Marcos Antonio Vaz Salles, Zongyang
            Zhang, Tong Li, Bin Hu, Fritz Henglein, and Rongxing Lu. Building
            Blocks of Sharding Blockchain Systems: Concepts, Approaches, and
            Open Problems, 2021. `https://arxiv.org/abs/2102.13364`.

[Nak09]   Satoshi Nakamoto. Bitcoin: A Peer-to-Peer Electronic Cash System,
            2009. `https://bitcoin.org/bitcoin.pdf`.

[Pag20]   Emiliano Pagnotta. Decentralizing Money: Bitcoin Prices and
            Blockchain Security, 2020. `https://papers.ssrn.com/sol3/`
            `papers.cfm?abstract_id=3152803`.

[PB18]   Emiliano Pagnotta and Andrea Buraschi. An Equilibrium Valuation
            of Bitcoin and Decentralized Network Assets, 2018. `https://`
            `papers.ssrn.com/sol3/papers.cfm?abstract_id=3142022`.

[Pla26]   Rutherford H. Platt Jr. The Forgotten Books of Eden: Book of
            Secrets of Enoch, 1926. `https://www.sacred-texts.com/bib/`
            `fbe/fbe129.htm`.

[PS16]   Rafael Pass and Elaine Shi. Hybrid Consensus: Efficient Consensus
            in the Permissionless Model. Cryptology ePrint Archive, Report
            2016/917, 2016. `https://eprint.iacr.org/2016/917`.

[RC06]   HariGovind V. Ramasamy and Christian Cachin. Parsimonious
            Asynchronous Byzantine-Fault-Tolerant Atomic Broadcast. Cryp-
            tology ePrint Archive, Report 2006/082, 2006. `https://eprint.`
            `iacr.org/2006/082`.

[RGK19]   Mayank Raikwar, Danilo Gligoroski, and Katina Kralevska. SoK
            of Used Cryptography in Blockchain. Cryptology ePrint Archive,
            Report 2019/735, 2019. `https://eprint.iacr.org/2019/735`.

[RMD+20]   Tayebeh Rajab, Mohammad Hossein Manshaei, Mohammad Dakhi-
            lalian, Murtuza Jadliwala, and Mohammad Ashiqur Rahman. On
            the Feasibility of Sybil Attacks in Shard-Based Permissionless
            Blockchains, 2020. `https://arxiv.org/abs/2002.06531`.

[SJS+21]   Nicholas Stifter, Aljosha Judmayer, Philipp Schindler, Andreas
            Kern, and Walid Fdhila. What is Meant by Permissionless
            Blockchains? Cryptology ePrint Archive, Report 2021/023, 2021.
            `https://eprint.iacr.org/2021/023`.

[SSVK20]   Savva Shanaev, Arina Shuraeva, Mikhail Vasenin, and Maksim
            Kuznetsov. Cryptocurrency Value and 51% Attacks: Evidence
            from Event Studies, 2020. `https://doi.org/10.3905/jai.2019.`
            `1.081`.