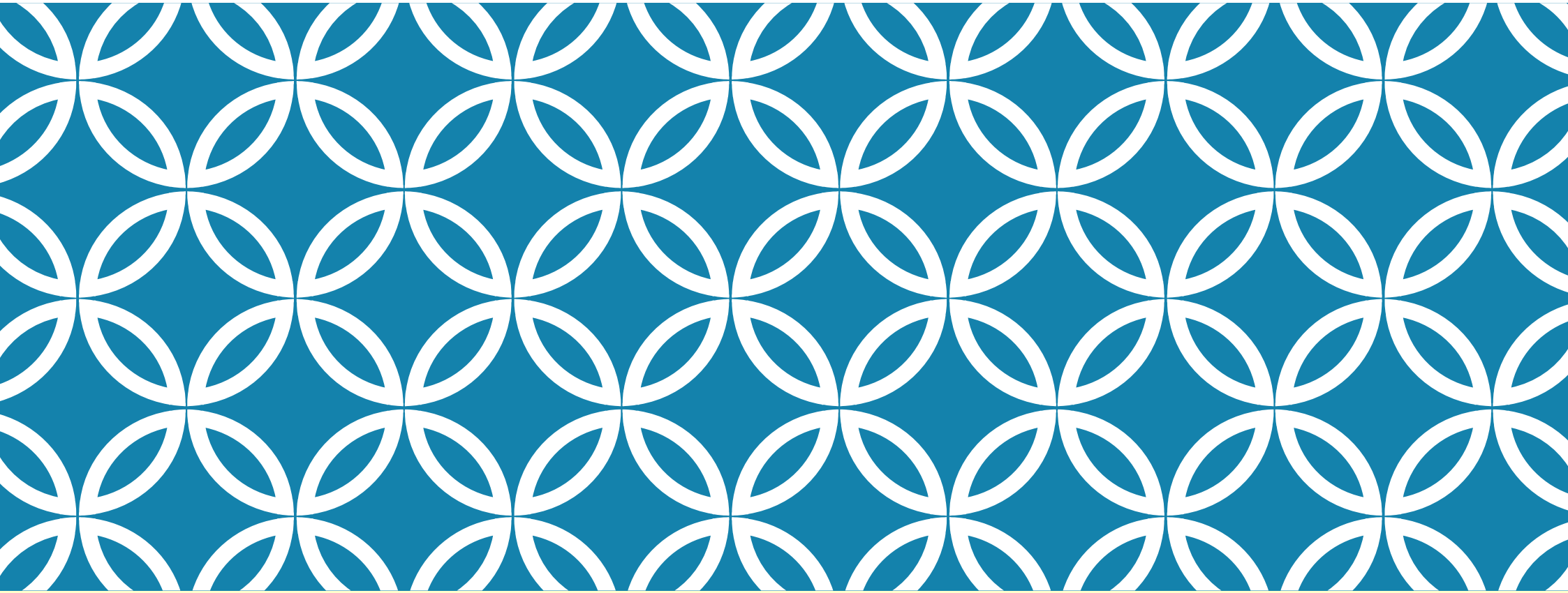
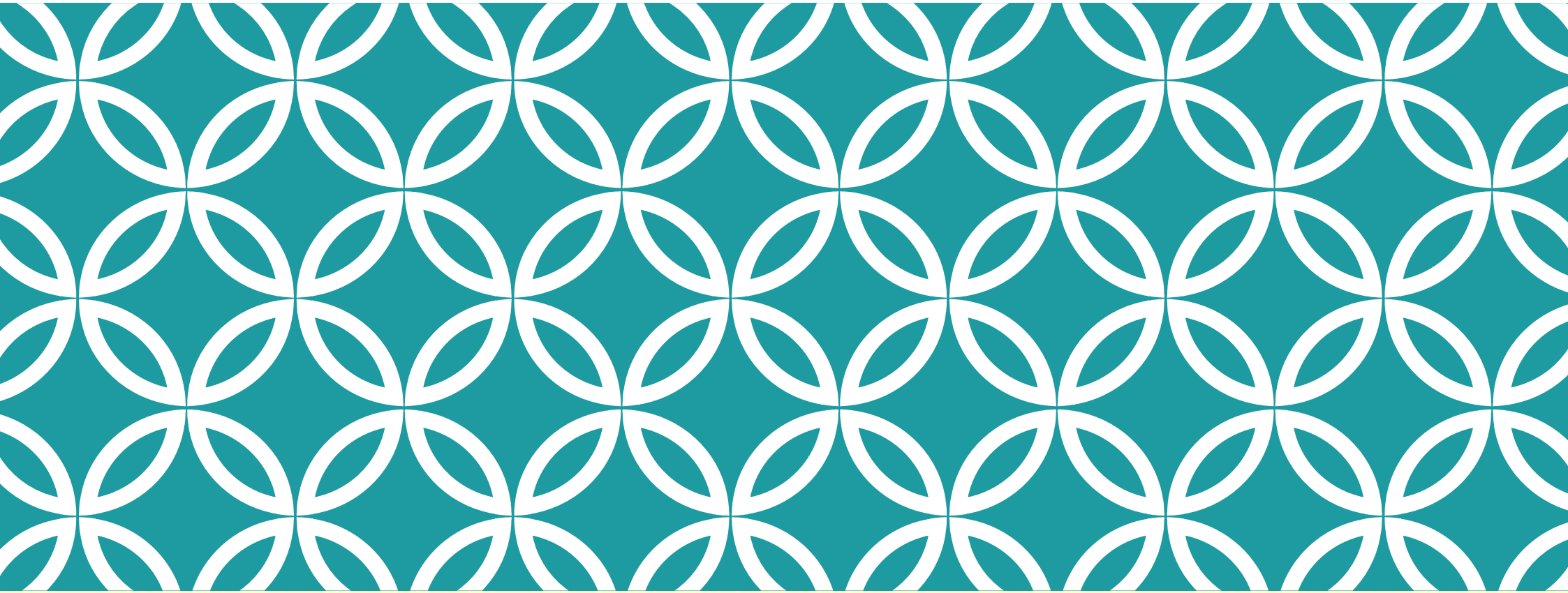


# 技术范式与中心化

A technical explaination of centralization in Ethereum Protocol

- 一些政治学
- 以太坊协议中的中心化因子
- 历史事件回顾
- 附录：比特币的开发哲学



# 一些政治学

Views from policitcs

# （一）亚里士多德

- 三种政治制度以及它们的堕落形式
  - 君主制 ———> 暴君制
  - 贵族制 ———> 寡头制
  - 民主制 ———> 暴民制

# （二）卢梭

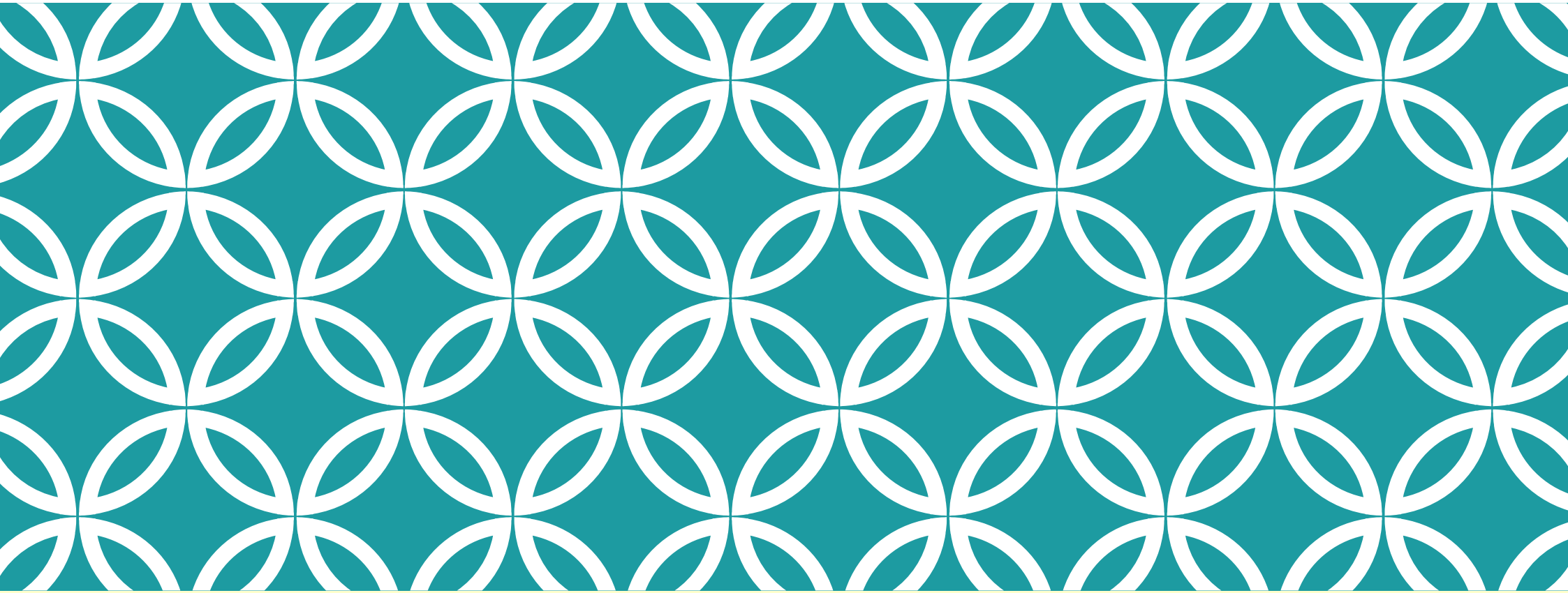
- 自然状态与社会契约
  - “主权”与“公共意志（公意）”
  - “人民主权”vs.“民主”

## （三）孟德斯鸠

- 三权分立（立法、行政、司法）

# （四）以赛亚·伯林

- 积极自由 vs. 消极自由
  - “谁能统治我”vs.“统治我到什么份上”



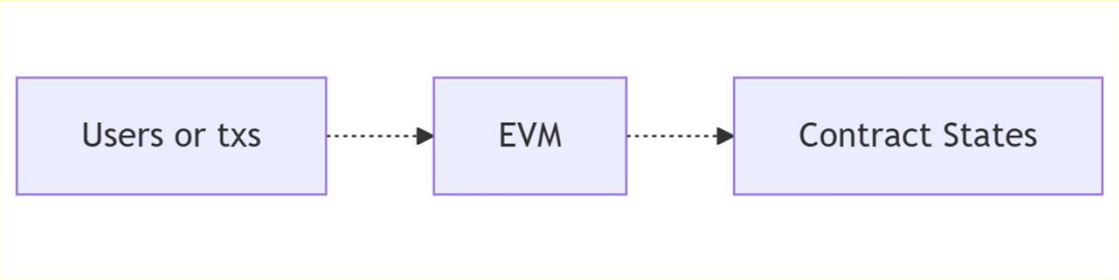
# 以太坊协议中的中心化因子

Centralization in Ethereum Protocol

# （一）以太坊协议

- “图灵完备”
  - 可以编程任意计算
  - 如何约束计算的资源消耗?
- 全局状态（global state or uniform state）
  - 账户模式
  - 智能合约账户可以存储状态
- 富状态性（statefulness）
  - 智能合约账户之间可以相互访问
    - 而且访问次数仅受交易所指定的 Gas 数量限制

# （一）以太坊协议




对状态达成共识意味着不仅要对交易（操作码）的计算语义达成共识，还要对这些操作码的 Gas 消耗量达成严格的共识。

否则，在交易处理完成后，外部账户的 ETH 数量将不一致（共识崩溃）。

# （二）那么升级呢？

- 状态膨胀
  - 外部账户及合约账户的状态都会不断积累，使状态访问的操作码的 Gas 定价倾向于低估，鼓励滥用
  - 2019 伊斯坦布尔硬分叉，EIP-1884
  - 2021 柏林硬分叉，EIP-2929/2930

# （二）那么升级呢？

- “新功能”
  - 创建新的合约 创建/交互 方式
    - 2018 君士坦丁堡硬分叉，EIP-1014，CREATE2
  - 改变可能具有前景的 密码原语（crypto primitives）/计算 的 Gas 消耗量（经济性）
    - 2017 拜占庭硬分叉，EIP-196/197/198，zk-SNARKs & RSA

# （二）那么升级呢？

- 主动调整
  - 改变某种资源的定价（经济性）
    - 2019，伊斯坦布尔硬分叉，EIP-2028，CallData

# （二）那么升级呢？

- 主动调整
  - 改变某种资源的定价（经济性）
    - 2019，伊斯坦布尔硬分叉，EIP-2028，CallData

只有**硬分叉**！

# （三）硬分叉 VS. 软分叉

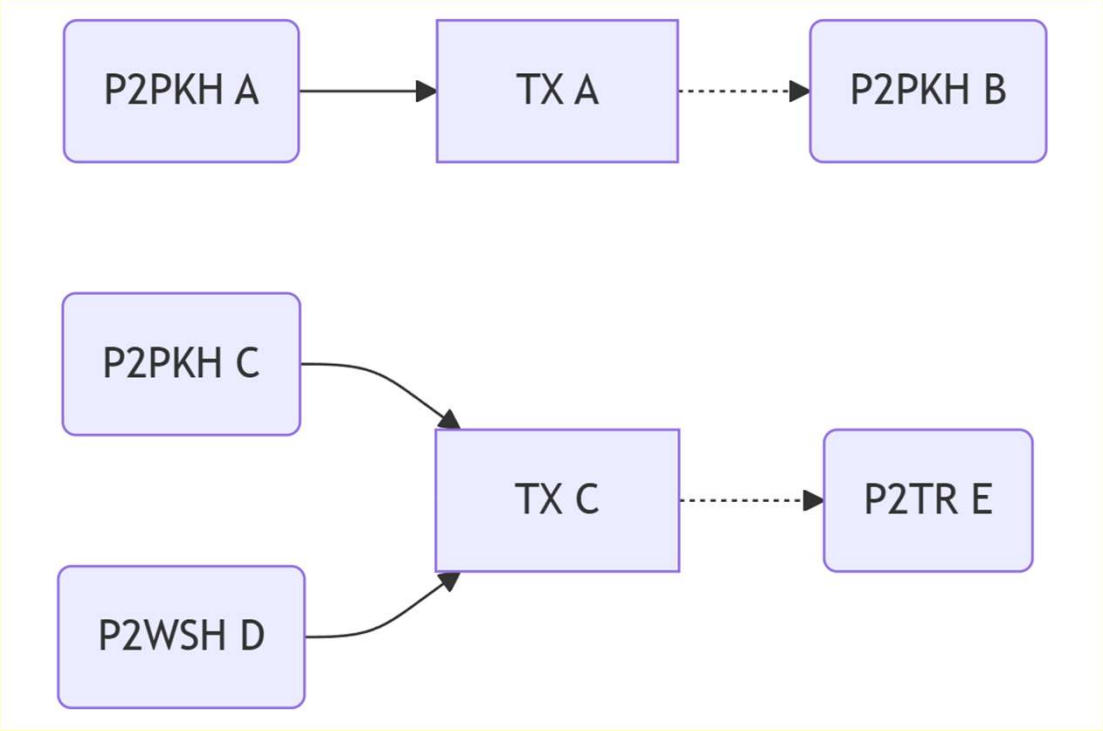
- 硬分叉：拓宽共识规则
  - 在原规则下无效的交易，在新规则下有效
  - 节点必须升级，否则会被抛离
- 软分叉：收窄共识规则
  - 原规则下有效的交易，新规则下不一定有效；但在新规则下有效的交易，在原规则下必定有效
  - 节点可以选择不升级，即依据原规则来验证，而不执行（由新规则定义的）额外验证

# （三）硬分叉 VS. 软分叉

- 在软分叉的世界里，全节点可以投“不信任票”，不升级，但依然用原有的共识规则来验证与自己有关的交易
- 但在硬分叉的世界里，全节点没有这个权利。
  - 如果你否决这次升级，你必须再造一个网络，来保留受此次升级影响的原有特性。

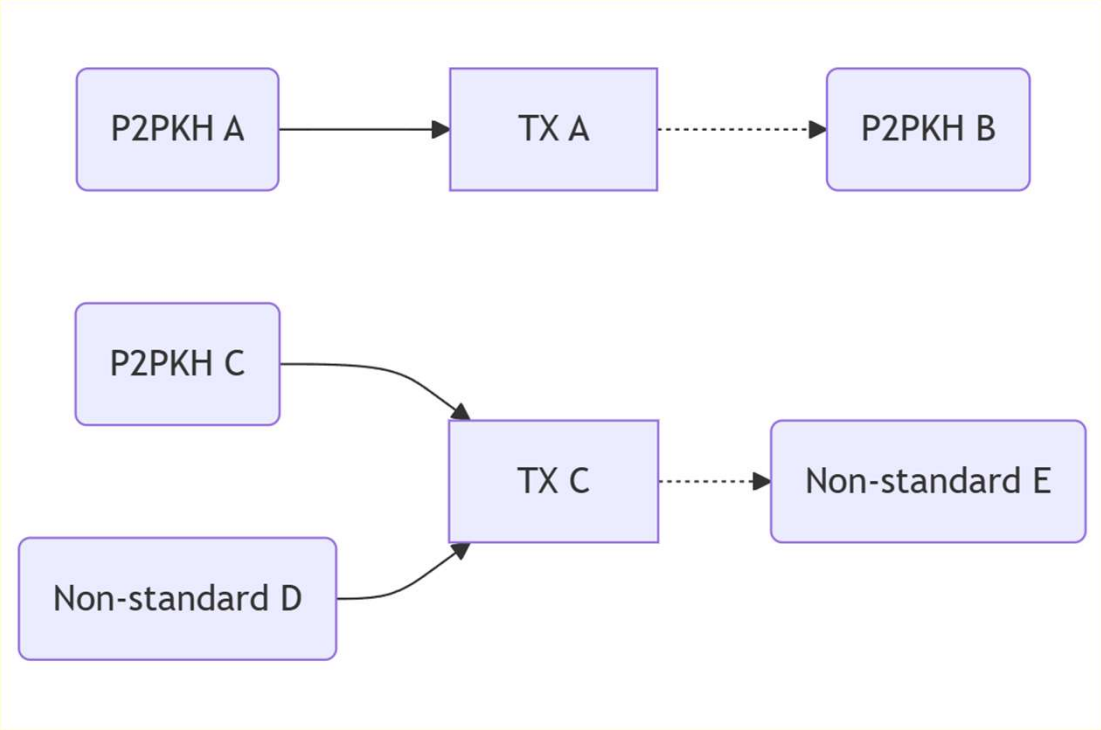
# 附录 A. 比特币 UTXO 与软分叉升级

对于理解 “Taproot 升级（Segwit v1）” 的节点来说：



# 附录 A. 比特币 UTXO 与软分叉升级

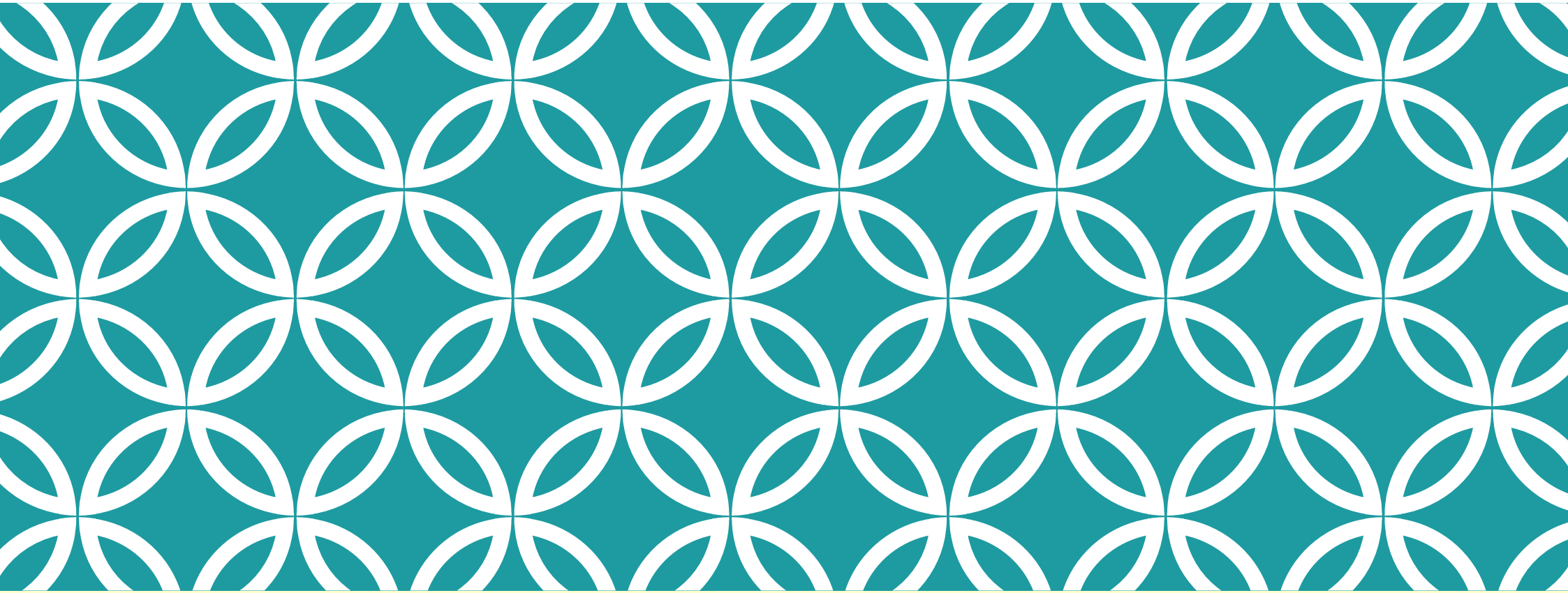
对甚至不理解“隔离见证（Segwit v0）”的节点来说：



# （四）硬分叉，GAS 定价与中心化

- 硬分叉打破了用户、开发者与矿工（出块者）的三权分立
- 在尝试衡量多种不同的资源时，Gas 定价并无科学标准可言，也不能保证不会再次改变
  - 这使资源的 Gas 重定价几乎总是一种（字面意义上的）政治决定

**所有导向中心化的因素都已经准备好，而且根植于以太坊协议本身。**



# 回顾历史

Events in Ethereum's history

# （一） HOW IT COMES

- “比特币 2.0”
  - PoW
  - “智能合约”
- 去中心化治理
  - EIP（Ethereum Improvement Proposals）
  - All Core Dev Meeting
  - 论坛（Ethereum Magicaians etc.）

# （二） HOW IT GOES

- “比特币 2.0”
  - PoW
    - 但带有 “难度炸弹”
  - “智能合约”
    - 并不采用 UTXO 架构，反而设计了一套劫持所有用户的架构

# （二） HOW IT GOES

- 去中心化治理
  - EIP（Ethereum Improvement Proposals）
  - All Core Dev Meeting
    - 带有议程设置机制（需要申请才能参与）
  - 论坛（Ethereum Magicaians etc.）
    - 似乎并不在乎反对意见

# （三）何为“CORE DEV”？

- 社交媒体上的“Ethereum core dev”
  - “当前为以太坊底层协议开发提供重大支持的人”（Hudson，2020）
    - 不是头衔、不能阻止自我授予、无法剥夺
- 混淆、污名
  - “Bitcoin Core developers” vs. “Ethereum Core dev”

# （四）“社会共识”

- Vitalik Buterin: A Proof of Stake Design Philosophy (2016)
- Vitalik Buterin: Hard Forks, Soft Forks, Defaults and Coercion (2017)

# （四）EIP-1559

- 提出于 2018 年
- 在 2020 年底突然加速
- 引用并不能证明其观点（也不完整）的论文
  - Tim Roughgarden：Transaction Fee Mechanism Design for the Ethereum Blockchain
- Tim Beiko：Why 1559?
- 2021 年 8 月，伦敦硬分叉

# （四）“社会共识”

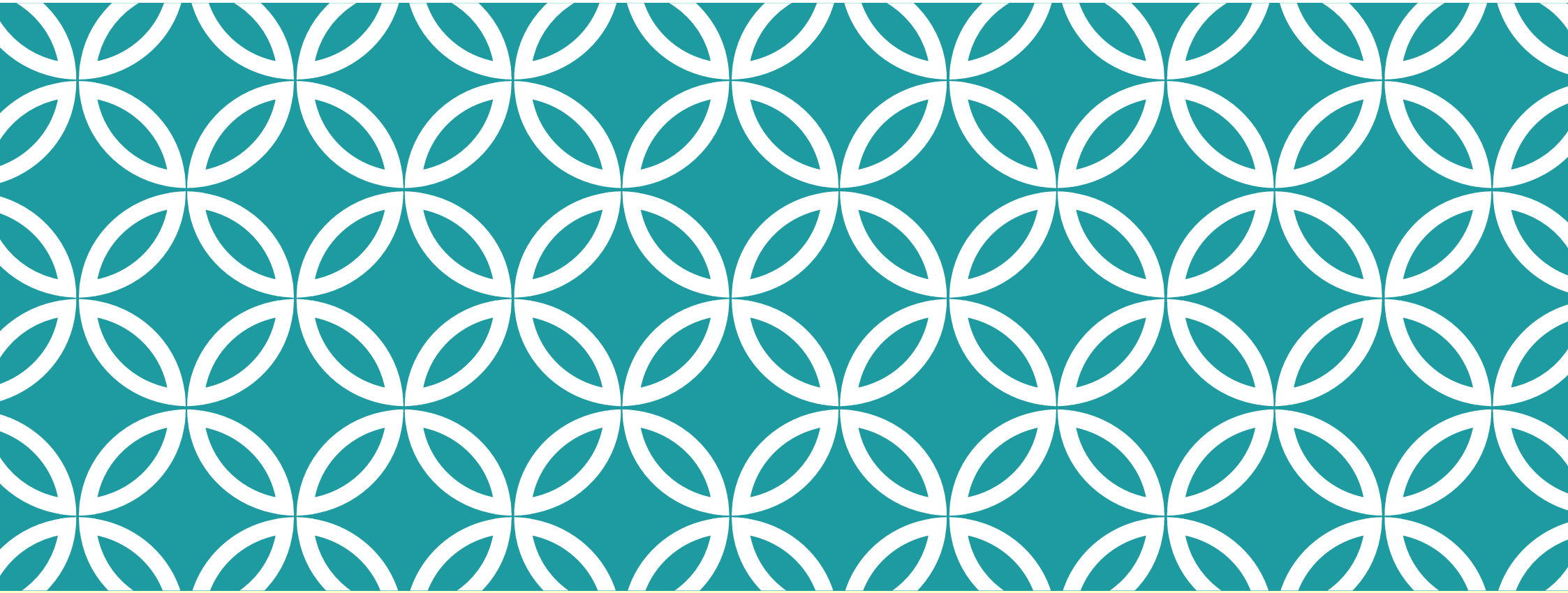
- Vitalik Buterin: The Most Important Scarce Resource is Legitimacy (2021)

# 附录 B. 比特币的开发·历史与现实

- 开源的软件开发（粗糙共识）
  - 曾经有过“仁慈独裁者”
- 没有路线图，只有原则
- 有以比特币为名的基金会（但它是做什么的呢？）
  - 不止一个 基金会/企业 在给最重要的比特币开发者提供经济支持（e.g. Blockstream、Chaincode、Brink...）
- 有过激烈的政治争议
- 最终来说，用户说了算

# 附录 B. 比特币的开发·原则

- 网络安全性
- 向后兼容性（软分叉）
- 无没收（使过去有效且可理解的用法作废）
- 免信任性
- 隐私性
- 不分裂



# 参考文献 | References

俞可平：最好政体与最坏政体，https://www.igcu.pku.edu.cn/info/1069/1547.htm

以赛亚·伯林：自由及其背叛，https://book.douban.com/subject/1437686/

孟德斯鸠：论法的精神，https://book.douban.com/subject/10876715/

以赛亚·伯林：自由论，https://book.douban.com/subject/6052799/

哈耶克：通往奴役之路，https://book.douban.com/subject/36141170/

精通以太坊，https://github.com/inoutcode/ethereum_book?tab=readme-ov-file

阿剑：“状态膨胀”与“无状态性”，https://github.com/editor-Ajian/Personal-Work/tree/main

Balaji S. Srinivasan: Quantifying Decentralization, https://news.earn.com/quantifying-decentralization-e39db233c28e

Hudson Jameson: What is an ethereum core developer?, https://hudsonjameson.com/2020-06-22-what-is-an-ethereum-core-developer/

原语里弄研究·难度炸弹简史，https://github.com/PrimitivesLane/Research/tree/main

0xB10C：不完整比特币开发史，https://www.btcstudy.org/2021/09/29/the-incomplete-history-of-bitcoin-development/

Jameson Lopp：比特币发生过硬分叉吗？，https://www.btcstudy.org/2022/09/02/has-bitcoin-ever-hard-forked/

Optech：比特币软分叉激活史，https://www.btcstudy.org/2021/09/29/soft-fork-activation-by-optech/

musclesatz：比特币的过去、现在与未来（四），https://www.btcstudy.org/2023/02/16/bitcoin-past-present-future-part-4/

Alex B.：比特币开发之道，https://www.btcstudy.org/2021/09/07/the-tao-of-bitcoin-development/

Jameson Lopp：比特币最重要的特性是哪些？，https://www.btcstudy.org/2022/08/05/what-are-the-key-properties-of-bitcoin/

Kalle Rosenbaum & Linnéa Rosenbaum: Bitcoin development philosophy，https://bitcoindevphilosophy.com/