A new ECDLP-based PoW model

A. Meneghetti, M. Sala, D. Taufer

University of Trento

DLT 2020
February 4th 2020

1. Useful PoW

A *proof of work* (PoW) demontrates to have spent a specific amount of computational work.

Pro's of a Bitcoin-like consensus algorithm:

- easily adjusteable workload with a fastly verifiable output
- easy to implement

Con's:

- huge amount of computations

Alternatives:

- Medical research (CureCoin)
- Data preservation (Permacoin)
- Micro-payment systems (Micromint)
- Research Propellant (Primecoin) $\longleftarrow$ We aim at this.

Our proposal:

- a blockchain architecture with a PoW-consensus algorithm based on the solution of the *Discrete Logarithm Problem* over the point groups of elliptic curves (ECDLP)

2. Full decentralization

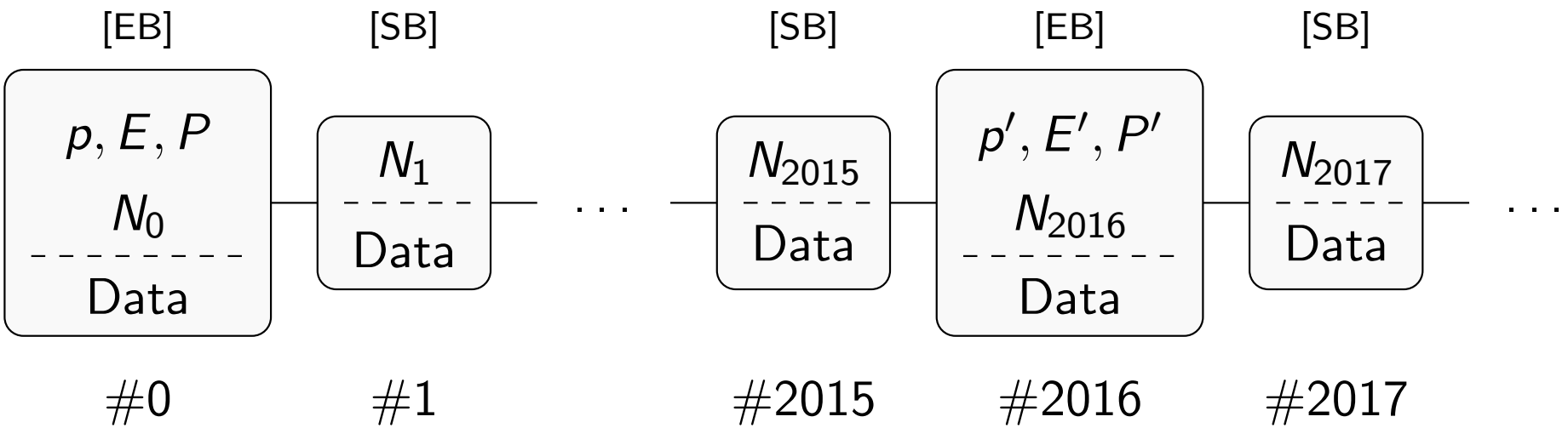
From *safecurves.cr.yp.to*:

"There are documented instances, and many more suspected instances, of standards being manipulated by attackers.
This raises the question of how users of standard curves can be assured that the curves were not generated to be weak."

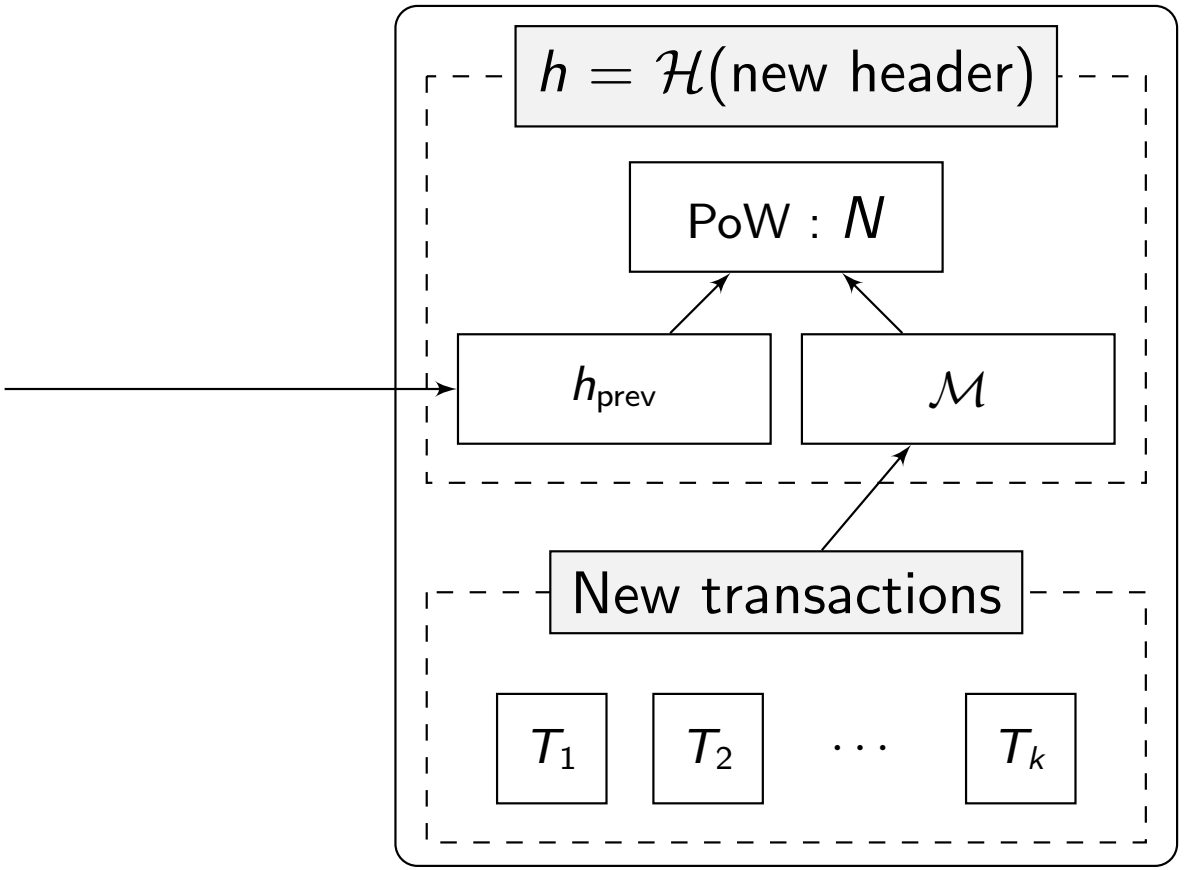
Rigidity levels

Fully rigid	⟵ We aim at this.
Somewhat rigid	Secp256k1 ("BTC Curve")
Manipulatable	NIST P-224, P-256, P-384
Trivially manipulatable	ANSSI FRP256v1

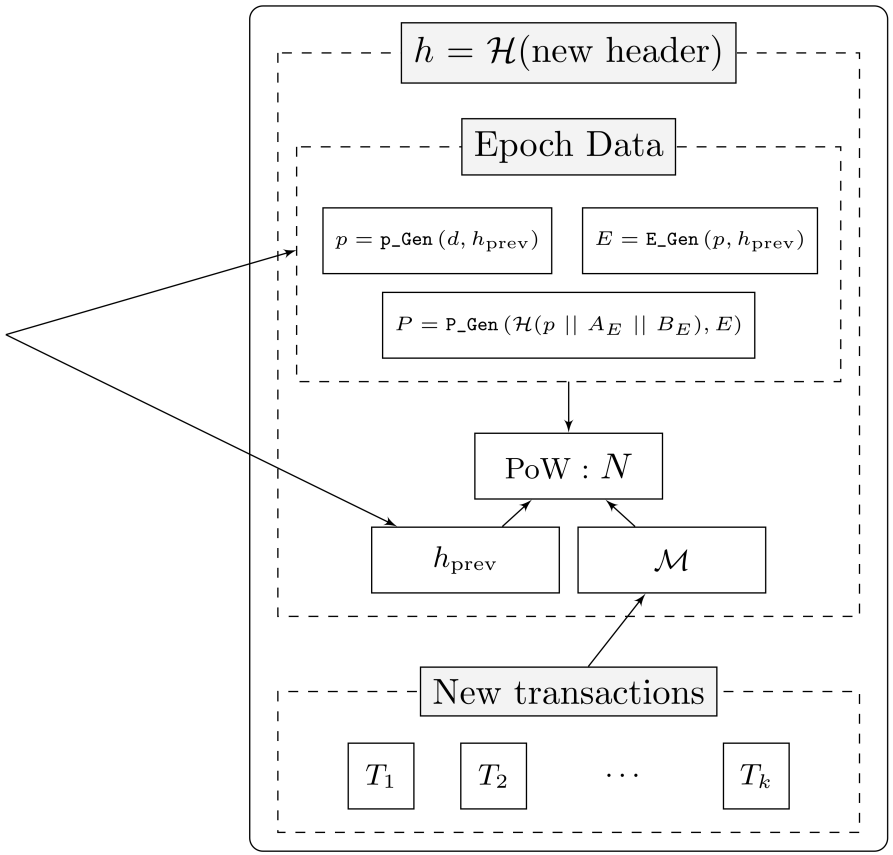
Blockchain Structure



Standard Blocks



Epoch Blocks



Security - Prime Numbers

The prime number p is the responsible of the expected run time of the PoW and its size is determined by a difficulty parameter d

EXCEPTIONALITY PROPERTIES

1. p is not a Crandall prime, i.e. not of the from $2^k - c$ for a relatively small and positive integer c.
2. p is neither a Generalized Mersenne prime nor a More Generalized Mersenne prime, i.e. it may not be written as $p(m)$ for some integer m and polynomial p with very small coefficients and number of monomials.
3. p is not Montgomery-friendly, i.e. it may not be obtained as $2^{\alpha}(2^{\beta} - \gamma) - 1$ for small positive integers α, β, γ.

Security - Elliptic Curves

We aim at generating pseudorandom elliptic curves for which no attacks are currently known

SECURITY PROPERTIES

1. The number of points of E is prime and different from p.
2. The *embedding degree* B is greater than 20, i.e. $|E| \nmid p^B - 1$ for every $1 \leq B \leq 20$.
3. Let D be the *CM field discriminant*, defined as

$$D = \begin{cases} \Delta & \text{if } \Delta \equiv 1 \bmod 4, \\ 4\Delta & \text{otherwise,} \end{cases} \qquad \Delta = \text{SquareFreePart}(t^2 - 4p),$$

where t is the trace of E. Then we require $D > 2^{40}$.

Security - Some Considerations

- Security based on the *generic* difficulty of the ECDLP, instead of DLP over fixed EC.
- Neither specific algorithms nor dedicated hardware may be used for solving such a general problem.
- *Fully rigid scheme*: even the system parameters are decided from the community.
- A strong hash funciton is needed.

Further Works

- Testing using PoC
- Further studies using Edwards or Montgomery curves
- Design similar PoW schemes using NP-C problems to address quantum attacks

Thank You All!