An attempt to give the most abstract possible definition of a blockchain.

1 BlockChain

1.1 Lists and their validation

Given a set S, let $\text{SET}(S)$ be the set of sets of elements of S and $\text{FLIST}(S)$ be the set of all finite lists of elements of S. Given $L \in \text{FLIST}(S)$, we use notation $\text{length}(L)$ to refer to the number of elements in L, notation $L[i]$ to refer to the i-th element in L, where $i \in \{1, \ldots, \text{length}(L)\}$, and notation $L[i, j]$ to refer to the sublist $[L[i], \ldots, L[j]]$ of L, where $i, j \in \{1, \ldots, \text{length}(L)\}$ and $i \leq j$. Notice that $\text{length}(L) = 0$ if and only if L is the empty list $[\,]$. Finally, we say that a list L_1 is a prefix of a list L_2 if L_1 is the empty list, or $1 \leq \text{length}(L_1) \leq \text{length}(L_2)$ and $L_1 = L_2[1, \text{length}(L_1)]$.

From now on, assume that Σ is a finite alphabet, and that $\mathbf{B} \subseteq \Sigma^*$ is the set of all possible blocks.

Definition 1. *A validation rule is a function* $V : \text{FLIST}(\mathbf{B}) \to \text{SET}(\mathbf{B})$

Intuitively, V is a function taking a finite list L of blocks as input, and returning the set of blocks that could be added to L to produce a valid blockchain.

A list $G \in \text{FLIST}(\mathbf{B})$ is said to be a genesis list of V if $\text{length}(G) \geq 1$, $G[1] \in V([\,])$ and $G[i+1] \in V(G[1, i])$, for every $i \in \{1, \ldots, \text{length}(G) - 1\}$. That is, G is a genesis list if G is a non-empty valid blockchain.

Definition 2. *Let V be a validation rule and G be a genesis list of V. Then a list $L \in \text{FLIST}(\mathbf{B})$ is valid with respect to (G, V) if:*

1. $\text{length}(G) \leq \text{length}(L)$ *and* $G = L[1, \text{length}(G)]$.
2. $L[i+1] \in V(L[1, i])$*, for every* $i \in \{\text{length}(G), \ldots, \text{length}(L) - 1\}$.

The role of G in this definition is to provide the blocks to startup the system. Let $\text{LOG}(G, V)$ be the set of valid lists with respect to (G, V).

Two lists $L_1, L_2 \in \text{FLIST}(\mathbf{B})$ are said to disagree in the last element if one of the following conditions holds: (1) $\text{length}(L_1) = 0$ and $\text{length}(L_2) > 0$, (2) $\text{length}(L_1) > 0$ and $\text{length}(L_2) = 0$, or (3) $\text{length}(L_1) > 0$, $\text{length}(L_2) > 0$ and $L_1[\text{length}(L_1)] \neq L_2[\text{length}(L_2)]$.

Definition 3. *Let V be a validation rule and G be a genesis list of V. Then $\text{LOG}(G, V)$ is safe if for every pair $L_1, L_2 \in \text{FLIST}(\mathbf{B})$ that disagree in the last element, it holds that $V(L_1) \cap V(L_2) = \emptyset$.*

1.2 Body of knowledge

In this document, we will give a game-theoretic characterization of the notion of blockchain where it plays a key role the knowledge of each participant. More precisely, given a validation rule V and a genesis list G of V, a body of knowledge of (G, V) is a non-empty and finite subset K of $\text{LOG}(G, V)$ satisfying the following closure property:

- if $L_1 \in \text{LOG}(G, V)$, L_1 is a prefix of L_2 and $L_2 \in K$, then $L_1 \in K$.

Intuitively, if at some iteration a participant considers a list $L \in \text{LOG}(G, V)$ as valid, then she should also consider as valid every prefix of L including the genesis list, that is, every prefix of L belonging to $\text{LOG}(G, V)$. The set of bodies of knowledge of (G, V) is denoted by $\text{BK}(G, V)$.

There is a natural way to visualize a body of knowledge K as a graph $\mathcal{G}(K)$. The set of nodes of $\mathcal{G}(K)$ is the set of blocks occurring in the lists in K, and there is an edge from a block b_1 to a block b_2 if there exists a list $L \in K$ such that $b_1 = L[i]$ and $b_2 = L[i+1]$, where $i \in \{1, \ldots, \text{length}(L) - 1\}$.

Lemma 1. *Assume that $\text{LOG}(G, V)$ is safe. Then for every $K \in \text{BK}(G, V)$, it holds that $\mathcal{G}(K)$ is a tree rooted at $G[1]$.*

1.3 Protocols and blockchain

Definition 4. *A relation $\preceq$ on* $\text{Log}(G, V)$ *is said to be a knowledge order over* (G, V) *if* $\preceq$ *is a total preorder on* $\text{Log}(G, V)$*, that is,* $\preceq$ *is reflexive, transitive and total.*

Moreover, a sequence $\{\preceq_i\}_{i \in \mathbb{N}}$ *is said to be a blockchain protocol over* (G, V) *if every* $\preceq_i$ $(i \in \mathbb{N})$ *is a knowledge order over* (G, V)*.*

Definition 5. *Let* $\{\preceq_i\}_{i \in \mathbb{N}}$ *be a blockchain protocol over* (G, V)*,* $K \in \text{BK}(G, V)$ *and* $t \in \mathbb{N}$*. Then a maximal element of* K *with respect to* $\preceq_t$ *is said to be a blockchain of* K *at iteration* t *with respect to the protocol* $\{\preceq_i\}_{i \in \mathbb{N}}$*.*

1.4 Definition of the game

Fix a validation rule V and a genesis list G of V. From now on, we assume that $\mathcal{P} = \{1, \ldots, n\}$ is a finite set of players, and we say that a view $\mathbf{v}$ is a tuple $(v_1, \ldots, v_n) \in \text{BK}(G, V)^n$. Intuitively, each component v_i of $\mathbf{v}$ represents the knowledge of player i, so $\mathbf{v}$ contains the knowledge of all the players. Moreover, we denote by $\mathcal{V}$ the set of all possible views, that is, $\mathcal{V} = \text{BK}(G, V)^n$.

Marcelo: Notice that I am using bold font for tuples. Please use the same notation in the rest of the paper.

Definition 6. *Given a player* $p \in \mathcal{P}$*, a function* $a : \mathcal{V} \to \mathcal{V}$ *is an action for* p *if*

- *for every* $\mathbf{v} \in \mathcal{V}$ *and* $q \in \mathcal{P}$*, if* $\mathbf{v} = (v_1, \ldots, v_n)$ *and* $a(\mathbf{v}) = (w_1, \ldots, w_n)$*, then it holds that:*

$$v_q \subseteq w_q \subseteq v_q \cup w_p.$$

Moreover, $\mathcal{A}_p$ *is the set of all actions for player* p*.*

An action of a player p is represented by a modification of the knowledge of p and a round of communication between players.

If we need to restrict the number of blocks that can be added when an action is executed (like in the case of Bitcoin), then we need to include in Definition 6 a condition like the following:

- for every $\mathbf{v} \in \mathcal{V}$, if $\mathbf{v} = (v_1, \ldots, v_n)$ and $a(\mathbf{v}) = (w_1, \ldots, w_n)$, then it holds that $|w_p| \leq |v_p| + 1$.

In this case, at most one block can be added as the result of executing action a by player p.

From now on, assume that $\mathcal{A} = \mathcal{A}_1 \times \mathcal{A}_2 \times \cdots \times \mathcal{A}_n$. Thus, every element of $\mathbf{a} \in \mathcal{A}$ is a tuple containing exactly one action for each player. Moreover, given a player $p \in \mathcal{P}$, a function $r_p : \mathcal{V} \times \mathcal{A} \to \mathbb{R}$ is called a reward function for p. Intuitively, given the knowledge of each player, encoded as a view $\mathbf{v}$ in $\mathcal{V}$, and the actions executed by each player, encoded as a tuple $\mathbf{a}$ in $\mathcal{A}$, function r_p tell us what the reward of player p is if the state of the world is v and the tuple of actions $\mathbf{a}$ is executed. Finally, assuming that there is a reward function r_p for each player $p \in \mathcal{P}$, define $\mathcal{R} = (r_1, \ldots, r_n)$ as the reward function of the game.

As a last component of the game, we assume that $\mathbf{Pr} : \mathcal{V} \times \mathcal{A} \times \mathcal{V} \to [0, 1]$ is a function such that for every $\mathbf{v} \in \mathcal{V}$ and $\mathbf{a} \in \mathcal{A}$:

$$\sum_{\mathbf{w} \in \mathcal{V}} \mathbf{Pr}(\mathbf{v}, \mathbf{a}, \mathbf{w}) = 1$$

Intuitively, $\mathbf{Pr}(\mathbf{v}, \mathbf{a}, \mathbf{w})$ tell us what the probability of modifying $\mathbf{v}$ to generate $\mathbf{w}$ is when the tuple of actions $\mathbf{a}$ is executed.

Then $\Gamma = (\mathcal{P}, \mathcal{A}, \mathcal{V}, \mathcal{R}, \mathbf{Pr})$ is an infinite stochastic game where :

- $\mathcal{P}$ is the set of player.
- $\mathcal{A}$ is the set of available action.
- $\mathcal{V}$ is the set of states.
- $\mathcal{R}$ the set of pay-off function.
- $\mathbf{Pr}$ is the transition probability function.

1.5 Stationary equilibrium

Definition 7. *We call stationary strategy for a player p a function $s : \mathcal{V} \to \mathcal{A}_p$ Moreover $\mathcal{S}_p$ is the set of all strategy for player p.*

From now on, assume that $\mathcal{S} = \mathcal{S}_1 \times \mathcal{S}_2 \times \cdots \times \mathcal{S}_n$. Thus, every element of $\mathbf{s} \in \mathcal{S}$ is a tuple containing exactly one strategy for each player.

Considering a view $\mathbf{v} \in \mathcal{V}$ and $\mathbf{s} \in \mathcal{S}$ we denote $\mathbf{s}(\mathbf{v})$ the action vector $(s_1(\mathbf{v}), \ldots, s_n(\mathbf{v})) \in \mathcal{A}$

Property 1. *Considering a game Γ and a stationary strategy vector $\mathbf{s} \in \mathcal{S}$, the probability to reach a view $\mathbf{v} \in \mathcal{V}$ in n step called n-reachability probability noted $\mathcal{P}^{\mathbf{s}}_n : \mathcal{V} \to [0; 1]$ is computed by induction :*

$$\mathcal{P}^{\mathbf{s}}_0(\mathbf{v}) = \begin{cases} 1 & \textit{if } \mathbf{v} = \mathbf{v}_0 \\ 0 & \textit{otherwise} \end{cases}$$

$$\mathcal{P}^{\mathbf{s}}_{n+1}(\mathbf{v}) = \sum_{\mathbf{v}' \in \mathcal{V}} \mathcal{P}^{\mathbf{s}}_n(\mathbf{v}') * \mathbf{Pr}(\mathbf{v}', \mathbf{s}(\mathbf{v}'), \mathbf{v})$$

Proof. immediate. □

Definition 8. *Let $\beta \in [0, 1]$, we call β discounted reward of player $p \in \mathcal{P}$ for a strategy vector $\mathbf{s} \in \mathcal{S}$ and a game Γ the value*

$$u_p(\mathbf{s}) = \sum_{n=0}^{+\infty} \beta^{n+1} * (\sum_{\mathbf{v} \in \mathcal{V}} r_p(\mathbf{v}, \mathbf{s}(\mathbf{v})) * \mathbf{Pr}(\mathbf{v}, \mathbf{s}(\mathbf{v}), s_p(\mathbf{v})) * \mathcal{P}^{\mathbf{s}}_n(\mathbf{v}))$$

Considering $p \in \mathcal{P}$, $\mathbf{s} \in \mathcal{S}$ and $s' \in \mathcal{S}_p$ we denote $(\mathbf{s}_{\neg p}, s')$ the strategy vector $(s_1, \ldots s_{p-1}, s', s_{p+1}, \ldots, s_n)$.

Definition 9. *We say that $\mathbf{s} \in \mathcal{S}$ is a β discounted stationary equilibrium of Γ iff :*

$$\forall p \in \mathcal{P}, \forall s' \in \mathcal{S}_p, u_p(\mathbf{s}) \geq u_p((\mathbf{s}_{\neg p}, s'))$$

1.6 Properties of a blockchain

Lemma 2. *Considering a game Γ and a stationary strategy vector $\mathbf{s} \in \mathcal{S}$, the probability to reach an element of a set of view $\mathbf{V} \in \textsc{Set}(\mathcal{V})$ without walking by an element of $\mathbf{V}' \in \textsc{Set}(\mathcal{V})$ in n steps noted $\mathcal{P}^{\mathbf{s}+}_n : \textsc{Set}(\mathcal{V}) \times \textsc{Set}(\mathcal{V}) \to [0; 1]$ is computed by induction :*

$$\mathcal{P}^{\mathbf{s}+}_0(\mathbf{V}, \mathbf{V}') = \begin{cases} 1 & \textit{if } \mathbf{v}_0 \in \mathbf{V} \\ 0 & \textit{otherwise} \end{cases}$$

$$\mathcal{P}^{\mathbf{s}+}_{n+1}(\mathbf{V}, \mathbf{V}') = \sum_{\mathbf{w} \in \mathcal{V} \setminus \mathbf{V}'} [\mathcal{P}^{\mathbf{s}+}_n(\{\mathbf{w}\}, \mathbf{V}') * \sum_{\mathbf{v} \in \mathbf{V}} \mathbf{Pr}(\mathbf{w}, \mathbf{s}(\mathbf{w}), \mathbf{v})]$$

Proof. to do. □

Lemma 3. *Considering a game Γ and a stationary strategy vector $\mathbf{s} \in \mathcal{S}$, the probability to reach an element of a set of view $\mathbf{V} \in \textsc{Set}(\mathcal{V})$ for the first time in n-step is equal to $\mathcal{P}^{\mathbf{s}+}_n(\mathbf{V}, \mathbf{V})$*

Proof. immediate. □

Property 2. *Considering a game Γ and a stationary strategy vector $\mathbf{s} \in \mathcal{S}$, the probability to reach an element of a set of view $\mathbf{V} \in \textsc{Set}(\mathcal{V})$ noted $\mathcal{P}^{\mathbf{s}} : \textsc{Set}(\mathcal{V}) \to [0; 1]$ is equal to*

$$\mathcal{P}^{\mathbf{s}}(\mathbf{V}) = \sum_{n=0}^{+\infty} \mathcal{P}^{\mathbf{s}+}_n(\mathbf{V}, \mathbf{V})$$

Proof. to do. $\square$

Definition 10. *Let P be a property over a view, let $\mathbf{v} \in \mathcal{V}$ we denote $\mathbf{v} \vdash P$ if $\mathbf{v}$ satisfies the property P. Let $\mathbf{V} \in \text{SET}(\mathcal{V})$ we denote $\mathbf{V} \vdash P$ if and only if $\forall \mathbf{v} \in \mathbf{V}, \mathbf{v} \vdash P$.*

Definition 11. *Considering (G, V), $\{\preceq_i\}_{i \in \mathbb{N}}$ a blockchain protocol over (G, V) and $\Gamma = (\mathcal{P}, \mathcal{A}, \mathcal{V}, \mathcal{R}, \mathbf{Pr})$ a stochastic game. We say that a property P is verified by (G, V), $\{\preceq_i\}_{i \in \mathbb{N}}$ regarding Γ with a probability α if and only if:*

- *Exists a β discounted stationary equilibrium of Γ*

- *Forall β discounted stationary equilibrium of Γ $\mathbf{s} \in \mathcal{S}$ for every set of view $\mathbf{V} \in \mathcal{V}$ we have*

$$\mathcal{P}^{\mathbf{s}}(\mathbf{V}) \geq \alpha \implies \mathbf{V} \vdash P$$

2 Block Equivalence

2.1 Equivalent Body of knowledge

Definition 12. *Given a validation rule V, a genesis list G of V and an equivalence relationship $\equiv$ over* **B**. *We say that $K_1 \in \text{BK}(G, V)$ and $K_2 \in \text{BK}(G, V)$ are $\equiv$ equivalent if and only if:*

$$\forall L_1 \in K_1, \exists L_2 \in K_2, \forall i \in [\![1, |L_1|]\!], L_1[i] \equiv L_2[i]$$
$$\forall L_2 \in K_2, \exists L_1 \in K, \forall i \in [\![1, |L_2|]\!], L_1[i] \equiv L_2[i]$$

By extension we denote $K_1 \equiv K_2$ resp. $L_1 \equiv L_2$ when two body knowledge resp. list are $\equiv$ equivalent.

We denote $\text{BK}^{\equiv}(G, V)$ the set of equivalence classes of $\text{BK}(G, V)$

Definition 13. *Given a validation rule V, a genesis list G of V and $\{\preceq_i\}_{i \in \mathbb{N}}$ a blockchain protocol over (G, V) we say that an equivalence relationship $\equiv$ over* **B** *is $\{\preceq_i\}_{i \in \mathbb{N}}$ compatible if and only if:*

$$\forall K_1, K_2 \in \text{BK}(G, V)$$

$$K_1 \equiv K_2 \implies \forall i \in \mathbb{N}, \forall L_1 \in \{L | L \in K_1, \forall L' \in K_1, L' \preceq_i L\}, \exists L_2 \in \{L | L \in K_2, \forall L' \in K_2, L' \preceq_i L\}, L_1 \equiv L_2$$

2.2 Game with equivalence

For now on we consider a game $\Gamma = (\mathcal{P}, \mathcal{A}, \mathcal{V}, \mathcal{R}, \mathbf{Pr})$ associated to a validation rule V a genesis list G and a blockchain protocol $\{\preceq_i\}_{i \in \mathbb{N}}$.

We say that two view $\mathbf{v}_1, \mathbf{v}_2 \in \mathcal{V}$ are equivalent regarding $\equiv$ a equivalent relationship over **B** noted $\mathbf{v}_1 \equiv \mathbf{v}_2$ if

$$\forall p \in \mathcal{P}, v_{1p} \equiv v_{2p}$$

We denote $\mathcal{V}^{\equiv}$ the set of equivalence classes of $\mathcal{V}$

Definition 14. *Let $\equiv$ a equivalence relationship over* **B** *we say that $\equiv$ is $\mathcal{A}$ compatible if $\forall p \in \mathcal{P}$ and $\forall a \in \mathcal{A}_p$ we have*

$$\forall \mathbf{v}_1, \mathbf{v}_2 \in \mathcal{V}, \mathbf{v}_1 \equiv \mathbf{v}_2 \implies a(\mathbf{v}_1) \equiv a(\mathbf{v}_2)$$

Definition 15. *Let $p \in \mathcal{P}$,considering $a_1, a_2 \in \mathcal{A}_p$ and $\equiv$ a equivalence relationship $\mathcal{A}$ compatible we say that a_1 and a_2 are equivalent noted $a_1 \equiv a_2$ if and if:*

$$\forall \mathbf{v}_1, \mathbf{v}_2 \in \mathcal{V}, \mathbf{v}_1 \equiv \mathbf{v}_2 \implies a_1(\mathbf{v}_1) \equiv a_2(\mathbf{v}_2)$$

We denote $\mathcal{A}_p^{\equiv}$ the set of equivalence classes of $\mathcal{A}$ then a element of $\mathcal{A}_p^{\equiv}$ is a function

$$a^{\equiv} : \mathcal{V}^{\equiv} \to \mathcal{V}^{\equiv}$$

.

Property 3. *Let $p \in \mathcal{P}$, $\equiv$ a equivalence relationship $\mathcal{A}$ compatible and $a^{\equiv} \in \mathcal{A}_p^{\equiv}$ then*

- *for every $\mathbf{v}^{\equiv} \in \mathcal{V}^{\equiv}$ and $q \in \mathcal{P}$, if $\mathbf{v}^{\equiv} = (v_1^{\equiv}, \ldots, v_n^{\equiv})$ and $a^{\equiv}(\mathbf{v}^{\equiv}) = (w_1^{\equiv}, \ldots, w_n^{\equiv})$, then it holds that:*

$$\forall v_q \in v_q^{\equiv}, \forall w_q \in w_q^{\equiv}, \forall w_p \in w_p^{\equiv}, v_q \ \subseteq \ w_q \ \subseteq \ v_q \cup w_p.$$

Proof. to do. □

Property 4. *Let $p \in \mathcal{P}$, and $\equiv$ a $\mathcal{A}$ compatible equivalence relationship over $\mathbf{B}$ then the function $\mathbf{Pr}^{\equiv}$: $\mathcal{V}^{\equiv} \times \mathcal{A}^{\equiv} \times \mathcal{V}^{\equiv} \to [0, 1]$ such that:*

$$\mathbf{Pr}^{\equiv}(\mathbf{v}^{\equiv}, \mathbf{a}^{\equiv}, \mathbf{w}) = \sum_{\mathbf{a} \in \mathbf{a}^e quiv} \mathbf{Pr}(\mathbf{v}, \mathbf{a}, \mathbf{w}) \textit{ where : } \mathbf{v} \in \mathbf{v}^{\equiv} \textit{ and } \mathbf{w} \in \mathbf{w}^{\equiv}$$

is well defined and

$$\forall \mathbf{v}^{\equiv} \in \mathcal{V}^e quiv, \forall \mathbf{a} \in \mathcal{A}^{\equiv}, \sum_{\mathbf{w}^{\equiv} \in \mathcal{V}^{\equiv}} \mathbf{Pr}^{\equiv}(\mathbf{v}^{\equiv}, \mathbf{a}^{\equiv}, \mathbf{w}^{\equiv}) = 1$$

Proof. to do. □

Definition 16. *Let $\equiv$ a equivalence relationship over $\mathbf{B}$ we say that $\equiv$ is $\mathcal{R}$ compatible if its $\mathcal{A}$ compatible and $\forall p \in \mathcal{P}$ and $\forall \mathbf{v} \in \mathcal{V}$ we have*

$$\forall \mathbf{a}_1, \mathbf{a}_2 \in \mathcal{A}, \mathbf{a}_1 \equiv \mathbf{a}_2 \implies r_p(\mathbf{v}, \mathbf{a}_1) = r_p(\mathbf{v}, \mathbf{a}_1)$$

Property 5. *Let $p \in \mathcal{P}$, and $\equiv$ a $\mathcal{R}$ compatible equivalence relationship over $\mathbf{B}$ then the function $r_p^{\equiv}$: $\mathcal{V}^{\equiv} \times \mathcal{A}^{\equiv} \to \mathbb{R}$ such that :*

$$r_p^{\equiv}(\mathbf{v}^{\equiv}, \mathbf{a}^{\equiv},) = r_p(\mathbf{v}, \mathbf{a}) \textit{ where : } \mathbf{v} \in \mathbf{v}^{\equiv} \textit{ and } \mathbf{a} \in \mathbf{a}^{\equiv}$$

is well defined.

Proof. to do. □

Property 6. *Let $\equiv$ a $\mathcal{R}$ compatible equivalence relationship over $\mathbf{B}$ then $\Gamma^{\equiv} = (\mathcal{P}, \mathcal{A}^{\equiv}, \mathcal{V}^{\equiv}, \mathcal{R}^{\equiv}, \mathbf{Pr}^{\equiv})$ is a well defined infinite stochastic game.*

Proof. immediate. □

3 Etienne 's modification space