

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

# 1 BlockChain

## Chains as lists and their validation

Given a set  $S$ , let  $\text{LIST}(S)$  and  $\text{SET}(S)$  be the sets of all finite lists and all finite sets of elements of  $S$ , respectively. Given  $L \in \text{LIST}(S)$ , we use notation  $|L|$  to refer to the number of elements in  $L$ , and notation  $L[i]$  to refer to the  $i$ -th element in  $L$ , where  $i \in \{1, \dots, |L|\}$ . From now on, assume that  $\Sigma$  is a finite alphabet, and that  $\mathbf{B} \subseteq \Sigma^*$  is the set of all possible blocks. Moreover we extend the definition of  $\subseteq$  such that :

$$\forall S \in \text{SET}(B), \forall L \in \text{LIST}(B), L \subseteq S \Leftrightarrow \forall i \in \{1, \dots, |L|\}, L[i] \in S$$

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

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

**Definition 2.** Let  $G \in \text{LIST}(\mathbf{B})$  be non-empty, and  $V$  be a validation rule. Then a list  $L \in \text{LIST}(\mathbf{B})$  is a validated chain with respect to  $(G, V)$  if:

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

List  $L$  in this definition is a valid chain according to the validation rule  $V$  and the lists  $G$  of genesis blocks (whose role is to provide the blocks to startup the system). Let  $\text{LOG}(G, V)$  be the set of validated chains with respect to  $(G, V)$ .

**Definition 3.** Let  $G \in \text{LIST}(\mathbf{B})$  be non-empty, and  $V$  be a validation rule. Then  $\text{LOG}(G, V)$  is safe if for every  $L \in \text{LOG}(G, V)$  such that every  $b_1, b_2 \in \mathbf{B}$  such that  $b_1 \neq b_2$ :

$$V([L[1], \dots, L[|L|], b_1]) \cap V([L[1], \dots, L[|L|], b_2]) = \emptyset$$

Intuitively, in order to be secured  $V$  should depend on the last block  $b$  that is included in the blockchain.

## Knowledge

**Definition 4.** A knowledge tree  $K$  is a tree  $K = (N, E)$  with  $N \subseteq \mathbf{B}$  and such that every path in  $K$  from its root to a leaf belongs to  $\text{LOG}_{G,V}$ . Let  $\mathcal{K}$  be the set of knowledge tree with respect to  $(G, V)$ .

Intuitively, the knowledge tree represents all the blockchain information we know. Abusing notation, we say that a block  $B$  is in a knowledge tree  $K = (N, E)$  if  $B \in N$ . (this is informal) We use  $\text{PATHS}(K)$  to denote the set of all lists of blocks made out of a path in  $K$  from its root to a leaf.

## Block chain, protocols

**Definition 5.** Let  $\preceq_{G,V,t}$  be a total preorder over  $\text{LOG}_{G,V}$ :

$$\begin{aligned} \forall L_1, L_2, L_3 \in \text{LOG}_{G,V}, L_1 \preceq_{G,V,t} L_2 \wedge L_2 \preceq_{G,V,t} L_3 &\implies L_1 \preceq_{G,V,t} L_3 \\ \forall L_1, L_2 \in \text{LOG}_{G,V}, L_1 \preceq_{G,V,t} L_2 \vee L_2 \preceq_{G,V,t} L_1 & \end{aligned}$$

A block chain protocol over  $\text{LOG}_{G,V}$  is a function noted  $\preceq_{G,V}$  such that:

$$\forall t \in \mathbb{N}, \preceq_{G,V}(t) = \preceq_{G,V,t}$$

where  $\preceq_{G,V,t}$  is a total preorder over  $\text{LOG}_{G,V}$

**Definition 6.** Let  $t \in \mathbb{N}$ ,  $\preceq_{G,V}$  a block chain protocol and  $K$  a knowledge tree. A block chain of  $K$  with respect to  $\preceq_{G,V}$  in  $t$  is any minimal element in  $\text{PATHS}(K)$  with respect to  $\preceq_{G,V}(t)$ .

## Action, incentive and game

**Definition 7.** We call action a function  $a : \mathcal{K} \rightarrow \mathcal{K}$  such that:

$$\begin{aligned} \forall K \in \mathcal{K}, K &\subseteq a(K) \\ \forall K \in \mathcal{K}, |a(K) \setminus K| &\leq 1 \end{aligned}$$

Let  $A$  be the set of action.

The action represents the mining strategy we only capture valid mining strategy... not sure if the second property is needed we could represent more complex strategy without it. Have to think about it.

**Remark.** In order to reach a finite number of action we might end up definition them over equivalence classes of  $K$  (meaning a block  $B$  upon  $V(L)$  is equivalent to mine a block  $B'$  upon  $V(L)$ ) then the number of possible action for a player would be  $|\text{Path}(K)|$ . just an idea that i dont want to forget.

**Definition 8.** We call incentive a function  $I : A \times \mathcal{K} \times P \rightarrow \mathbb{R}^+$

This incentive function will capture all the real world assumption such as, want money, destroy system ?, 50% hpower etc ... reward will also rely on probability to success.

**Definition 9.** Considering a set of player  $P$ , a function  $K_P : P \rightarrow \mathcal{K}$ , the set of action  $A$ , and a incentive  $I$ . We define a strategic game such that:

- $P$  is the set of player.
- $\forall p \in P$ ,  $A$  is the set of available action.
- $\forall p \in P, \forall a_1, a_2 \in A$  we say that  $a_1$  is preferred to  $a_2$  if  $I(a_1, K_P(p), p) \geq I(a_2, K_P(p), p)$ .

Tweak definition a bit to reach finite game (doable if i touch to  $A$ ) and prove equilibrium existence..

**Definition 10.** We say that  $K'_P$  is reasonable if exists an action  $a \in A$  associate to a player  $w \in P$  in an equilibrium profile such that:

$$\begin{aligned} K'_P(w) &= a(K_P(w)) \\ \forall p \in P, K_P(p) &\subseteq K'_P(p) \\ \forall p \in P, K'_P(p) &\subseteq K_P(p) \cup K'_P(w) \end{aligned}$$

$K'_P$  represent all the possible knowledge after one reasonable action (on belonging to a nash equilibrium) has happened with an optional communication round from the winner ( $K'_P(p) \subseteq K_P(p) \cup K'_P(w)$ ).

Good to go we finally have a definition of reasonable  $K$  and can define blockchain property which should be verified over all reasonable  $K$ .

## 2 old stuff

### Block chain game

**Definition 11.** A block-chain game is a tuple  $(G, V, \preceq_{G,V}, P, \mathcal{K}, D)$  where  $V$  is a validation rule,  $G$  a list of genesis blocks,  $\preceq_{G,V}$  a block chain protocol over  $LOG_{G,V}$ ,  $P$  a set of player,  $\mathcal{K}$  a function which map each player of  $P$  to a knowledge tree and  $D : P \rightarrow [0, 1]$  such that

$$\sum_{p \in P} D(p) = 1 \vee \sum_{p \in P} D(p) = 0$$

$D(p)$  represents the probability, that a player  $p$ , has to be the first to discover a list  $L \in LOG_{G,V}$  such that for all  $L'$  block chain of  $\mathcal{K}(p)$  with respect to  $\preceq_{G,V}(t)$ ,  $L \neq L'$  and  $L \preceq_{G,V,t} L'$

**Definition 12.** A block-chain game  $(G, V, \preceq_{G,V}, P, \mathcal{K}, D)$  is said to be alive if

$$\sum_{p \in P} D(p) = 1$$

### Strategies for discovery

**Definition 13.** A strategy is a partial function  $S : \mathbf{B} \times \mathbb{N} \rightarrow [0, 1]$  that satisfies  $S(B, i) \leq S(B, j)$  for all  $i \leq j$ . That is,  $S$  assigns to each block  $B$  and number  $i$  a probability  $S(B, i)$  that is not decreasing on  $i$ .

Intuitively, a strategy assigns to a time  $i$  a probability that a certain block is discovered amongst the  $i$  next blocks that are discovered.

**Definition 14.** Given a genesis  $G$  and a validation function  $V$ , A Knowledge representation for  $G$  and  $V$  is a pair  $(K, S)$ , where  $K$  is a knowledge tree and  $S$  is a strategy with preimage  $\{B \in \mathbf{B} \mid B \notin K\} \times \mathbb{N}$ .

Let  $\mathcal{K}$  be a set  $\{(K_1, S_1), \dots, (K_n, S_n)\}$  of knowledge trees. We say that  $LOG_{G,V}$  is alive with respect to  $\mathcal{K}$  if there is an  $(K_\ell, S_\ell)$  with  $1 \leq \ell \leq n$  and a block  $B$  not in  $K_\ell$  such that

$$\lim_{\delta \rightarrow +\infty} S_\ell(B, \delta) = 1$$

$LOG_{G,V}$  is alive with respect to  $\mathcal{K}$  and a protocol  $\preceq_{G,V}$  on a time  $t$  if there is an  $(K_\ell, S_\ell)$  with  $1 \leq \ell \leq n$  and a block  $B \in V(BC_t)$  such that

$$\lim_{\delta \rightarrow +\infty} S_\ell(B, \delta) = 1,$$

where  $BC_t$  is a blockchain of  $K_\ell$  with respect to  $\preceq_{G,V}$  in  $t$ .

**Definition 15.** Let  $P$  be a set of players and  $K_T$  a function :

$$K_T : P \times \llbracket 0; T \rrbracket \times \mathbb{N} \rightarrow \text{SET}(\mathbf{B} \times [0; 1])$$

Then  $(P, K_T)$  is a valid knowledge representation if :

$$\begin{aligned} \forall p \in P, \forall t \in \llbracket 0; T \rrbracket, (b, \alpha) \in K_T(t, 0, p) &\implies \alpha = 1 \vee \alpha = 0 \\ \forall p \in P, \forall t, t' \in \llbracket 0; T \rrbracket, t' \geq t, \forall b \in \mathbf{B}, (b, 1) \in K_T(t, 0, p) &\implies (b, 1) \in K(t', 0, p) \\ \forall p \in P, \forall t \in \llbracket 0; T \rrbracket, \forall \delta \in \mathbb{N}, \forall b \in \mathbf{B}, (b, 1) \in K_T(t, 0, p) &\implies (b, 1) \in K(t, \delta, p) \\ \forall p \in P, \forall t \in \llbracket 0; T \rrbracket, \forall \delta, \delta' \in \mathbb{N}, \delta' \geq \delta &\implies \forall (b, \alpha) \in K_T(p, t, \delta), \exists (b, \alpha') \in K_T(p, t, \delta'), \alpha' \geq \alpha \end{aligned}$$

**Notation.**  $\forall p \in P, \forall t \in \llbracket 0; T \rrbracket$  we denote

$$K_T(p, t) = \{b \mid (b, 1) \in K_T(p, t, 0)\}$$

**Definition 16.** Let  $T, T' \in \mathbb{N}$  such that  $T > T'$  we say that  $K'_{T'}$  extend  $K_T$  if

$$\forall p, K_T(p, T) = K'_{T'}(p, T)$$

**Definition 17.** Let  $\preceq_{G,V,t}$  be a total preorder over  $LOG_{G,V}$ :

$$\begin{aligned} \forall L_1, L_2, L_3 \in LOG_{G,V}, L_1 \preceq_{G,V,t} L_2 \wedge L_2 \preceq_{G,V,t} L_3 &\implies L_1 \preceq_{G,V,t} L_3 \\ \forall L_1, L_2 \in LOG_{G,V}, L_1 \preceq_{G,V,t} L_2 \vee L_2 \preceq_{G,V,t} L_1 & \end{aligned}$$

A block chain protocol over  $LOG_{G,V}$  is a function noted  $\preceq_{G,V}$  such that:

$$\forall t \in \mathbb{N}, \preceq_{G,V}(t) = \preceq_{G,V,t}$$

where  $\preceq_{G,V,t}$  is a total preorder over  $LOG_{G,V}$

**Remark.**  $\preceq_{G,V}$  can be seen as the rules in case of fork and new block.

**Definition 18.** Considering  $LOG_{G,V}$  the set of validated chains with respect to  $(G, V)$ ,  $(P, K_T)$  a valid knowledge representation and  $\preceq_{G,V}$  a block chain protocol. We denote  $S_{t,p}$  where  $t \in \llbracket 0, T \rrbracket$  and  $p \in P$  the set:

$$S_{t,p} = \{L | L \in LOG_{G,V} \wedge L \subseteq K_T(p, t)\}$$

We call a BlockChain at time  $t \in \llbracket 0, T \rrbracket$  for user  $p \in P$  noted  $BC_{t,p}$  a list such that:

$$BC_{t,p} \in S_{t,p} \wedge \forall L \in S_{t,p}, L \preceq_{G,V,t} BC_{t,p}$$

**Remark.** Intuitively the blockchain for a user  $p$  at a time  $t$  is one of the best chain he fully knows regarding the protocol function and the validity at time  $t$  (time-stamping).

**Definition 19.** Considering  $LOG_{G,V}$  the set of validated chains with respect to  $(G, V)$ ,  $(P, K_T)$  a valid knowledge representation. We denote  $\alpha^*$  the function

$$\mathbb{N} \times LOG_{G,V} \times P \rightarrow [0, 1]$$

such that :

$$\alpha^*(\delta, L, p) = \max\{\alpha | \exists b \in \mathbf{B}; (b, \alpha) \in K_T(p, T, \delta) \cap V(L)\}$$

We said that  $LOG_{G,V}$  is alive regarding  $(P, K_T)$  if:

$$\exists p \in P, \exists L \in LOG_{G,V}, L \subseteq K_T(p, T) \wedge K_T(p, T) \cap V(L) = \emptyset \wedge \lim_{\delta \rightarrow +\infty} \alpha^*(\delta, L, p) = 1$$

### 3 draft

**Definition 20.** Considering  $(P, K_T)$  a valid knowledge representation,  $LOG_{G,V}$  the set of validated chains with respect to  $(G, V)$  alive, and  $\preceq_{G,V}$  a block chain protocol. Let  $L \in LOG_{G,V}$  we note the probabilty that  $L \subseteq B_{T+\delta,p}$

**Definition 21.** Considering  $LOG_{G,V}$  the set of validated chains with respect to  $(G, V)$ ,  $(P, K_T)$  a valid knowledge representation. A block chain protocol  $\preceq_{G,V,T}$  is said to be ageing-secured if

$$\begin{aligned} \forall p \in P, \forall T_0 < T, \forall t, t' \leq T, B_{t,p} \subseteq B_{T_0,p}, B_{t',p} \subseteq B_{T_0,p} \\ t \leq t' \implies \forall T_1 \geq T_0, \mathbb{P}(B_{t,p} \subseteq B_{T_1,p}) \geq \mathbb{P}(B_{t',p} \subseteq B_{T_1,p}) \end{aligned}$$